Off the Grid:
Pinpointing Location-based Technologies and the Law

Written By:
Geoffrey White, Barrister & Solicitor
External Counsel
The Public Interest Advocacy Centre
1204 - ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

June 2015
Acknowledgement

Financial support from Industry Canada to conduct the research on which this report is based is gratefully acknowledged. The views expressed in this report are not necessarily those of Industry Canada or of the Government of Canada.

The author would also like to thank Kent Sebastian, PIAC Student-at-Law 2014-15, Sarah Mavula, PIAC Summer Student 2014, and Jonathan Bishop, PIAC’s Research & Parliamentary Affairs Analyst, for their research and contributions. Any mistakes are solely the author’s.
Executive Summary

Knowledge of the whereabouts of a person, and of a person’s movement patterns, can be very valuable, from a marketing perspective. Indeed, the scale and scope of the business opportunities associated with so-called location-based behavioural marketing and location-based services (collectively, location-based technologies) have been well-documented in the business literature. The opportunities for businesses to gain even more insights into consumer behaviour based on consumers’ whereabouts are said to be unprecedented given (i) the rapid growth in adoption and use by Canadians of smartphones and other mobile computing or “smart” devices with embedded global positioning system (GPS) chips, such as tablets; (ii) the rapid growth in adoption by businesses of Radio Frequency Identification (RFID) technology; and (iii) the increasing incorporation of location-based data into an increasing number of applications (apps) in use.

But are there issues in knowing where consumers are constantly? Will a balance be struck between the ability of retailers and others to reach consumers, via location-based advertising, and consumers’ desire to protect our privacy and keep the information collected about them secure? Are consumers sufficiently informed of how their location-based data is being used? Are their telecommunications service providers playing by the rules in terms of what information they are allowed to collect? Ultimately, the main research questions that this report aims to address are: Does the current legal and regulatory regime, which draws on elements of privacy law and telecommunications law, reflect broader social norms in respect of privacy? Do the legal, regulatory and self-regulatory approaches sufficiently protect consumers from the over-collection, misuse and inappropriate disclosure of their location-based personal information collected through mobile computing devices?

Through a detailed literature review and comparative analysis of other jurisdictions, a national telephone survey of consumer attitudes, and consultation with stakeholders and leading academics, the Public Interest Advocacy Centre (PIAC) has assessed the suitability of the legal and regulatory framework applicable to location-based technologies in light of Canadians’ attitudes and growing privacy concerns. Do the existing rules capture the types of location-based technology initiatives that are emerging, and are consumers sufficiently informed of when and how their location-based data is being used? Or are these initiatives “off the grid” – operating contrary to broader social norms of Canadian society?

This report outlines strong consumer concern over the collection and use of personal information, wide variation in collection and use practices by businesses, and a general lack of transparency of such practices. Therefore, it is essential that consumers have an effective legal framework to protect them from the rapid developments in information collection technology, especially those capturing location.

This report finds that location is an increasingly sought, increasingly tracked piece of information that can reveal much about individuals, and that Canadians are concerned about location-based
tracking. This report concludes that location about individuals should be considered highly sensitive personal information and should warrant strict legal protection. This report concludes that the contextual, principles-based approach to privacy in the federal privacy law (the Personal Information and Protection of Electronic Documents Act or “PIPEDA”) may not sufficiently protect Canadians from having information about their location over-collected (or surreptitiously collected), misused, and inappropriately disclosed, particularly by third parties.

Based on these conclusions, this report recommends that short of legislative reform, the federal privacy ombudsperson, the Office of the Privacy Commissioner of Canada (OPC), issue an Interpretation Bulletin addressing whether location information is personal information, and should conduct research into consumer awareness and expectations regarding location-based information collection use and disclosure. Finally, Canada’s telecommunications regulator, the Canadian Radio-television and Telecommunications Commission (CRTC), should initiate a fact-finding process into the tracking of location by telecommunications service providers, and their direct and indirect use of the collected location-based information generated from the use of their networks.
Table of Contents

Acknowledgement ........................................................................................................................ 3
Executive Summary ..................................................................................................................... 4
Glossary ....................................................................................................................................... 8
Chapter 1 – Introduction ............................................................................................................ 9
  The new rules of marketing: location, location, and… location ................................................. 9
  Growing privacy concerns ........................................................................................................ 11
  The issue: Do the current privacy rules adequately address location? ..................................... 14
Methodology ................................................................................................................................ 14
Why is this important? ................................................................................................................ 15
Report structure .......................................................................................................................... 16
Chapter 2 – Location-based technologies: an overview ............................................................. 17
  What is location? .................................................................................................................... 17
  What are Location-based Technologies? ................................................................................. 18
  Why is location information collected? .................................................................................. 21
    Technical reasons for collecting location information ......................................................... 21
    Public safety reasons for collecting location information .................................................... 21
    Commercial reasons for collecting location information ..................................................... 22
  How is location information collected? ................................................................................... 25
    Smartphone apps .............................................................................................................. 27
    Sensors ............................................................................................................................. 29
Examples of location-based technologies .................................................................................. 33
  Apple iOS location services ............................................................................................... 33
  Turnstyle Solutions ............................................................................................................. 34
  Via Informatics’s “LocationGenius” .................................................................................... 38
  iBeacon technology ........................................................................................................... 39
  Verizon Wireless Smart Rewards ...................................................................................... 42
  Canadian telecommunications service providers ............................................................... 43
Chapter 3 – Privacy concerns and consumer attitudes towards location-based technologies ...... 48
  Risks and concerns with location-based information tracking .................................................. 48
    Social concerns with behavioural profiling ..................................................................... 49
    Examples of specific harm ............................................................................................... 52
    The related risk: data vulnerability ................................................................................... 54
  Stakeholder views .................................................................................................................. 54
  What do Canadians think about location-based information privacy? ....................................... 56
    Prior consumer surveys .................................................................................................... 56
    The OPC’s Privacy Survey: 2014 .................................................................................... 57
# Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB-PIPA</td>
<td>Alberta’s <em>Personal Information Protection Act</em></td>
</tr>
<tr>
<td>BC-PIPA</td>
<td>British Columbia’s <em>Personal Information Protection Act</em></td>
</tr>
<tr>
<td>CRTC</td>
<td>Canadian Radio-television and Telecommunications Commission</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>GPS</td>
<td>Global positioning system</td>
</tr>
<tr>
<td>IPC-AB</td>
<td>Information and Privacy Commissioner of Alberta</td>
</tr>
<tr>
<td>IPC-BC</td>
<td>Information and Privacy Commissioner of British Columbia</td>
</tr>
<tr>
<td>LBM</td>
<td>Location-based marketing</td>
</tr>
<tr>
<td>IPC-ON</td>
<td>Information and Privacy Commissioner of Ontario</td>
</tr>
<tr>
<td>LBS</td>
<td>Location-based services</td>
</tr>
<tr>
<td>LBT</td>
<td>Location-based technologies (refers to both location-based marketing and location-based services)</td>
</tr>
<tr>
<td>MAC</td>
<td>Media access control</td>
</tr>
<tr>
<td>MLA</td>
<td>Mobile location analytics</td>
</tr>
<tr>
<td>OPC</td>
<td>Office of the Privacy Commissioner of Canada</td>
</tr>
<tr>
<td>PIPEDA</td>
<td><em>Personal Information Protection and Electronic Documents Act</em></td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-frequency identification</td>
</tr>
<tr>
<td>TSP</td>
<td>Telecommunications service provider</td>
</tr>
</tbody>
</table>
Chapter 1 – Introduction

The purpose of this report is to assess whether Canadian privacy law adequately protects Canadians from the collection, use and disclosure of information about their location generated by the heavy and growing use of mobile devices. In this report, “mobile devices” refers to cellular phones and mobile computing devices such as smartphones and tablets, and so-called “wearable” technology such as fitness trackers and “smartwatches.” The focus of this inquiry is on business-to-consumer relationships.¹

Mobile devices can, through a variety of hardware (e.g., global positioning system or GPS chips, radio-frequency identification or RFID chips) and software applications or “apps” (e.g., mapping services, fitness trackers), track the exact location of their users through time and share that information. In some cases the information is shared in ways initiated by and known to the user (e.g., letting a user’s social network know that he or she is at a given restaurant) and in other cases passively and unknown to the user (e.g., a free gaming app collecting location information, unrelated to the actual gameplay, or photos being automatically embedded with location data).² The ultimate use, including sharing of that information, is not always clear to consumers.

The new rules of marketing: location, location, and… location

In 2009, the Public Interest Advocacy Centre (PIAC) (and others) predicted that the rise of location-specific behaviourally-targeted marketing on mobile devices would be the next logical step for marketers.³ That same year, the Office of the Privacy Commissioner of Canada (OPC), which oversees Canada’s federal private-sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA),⁴ identified location data tracking as one of "three specific privacy concerns that are expected to become more important as the use of wireless

¹ There is also an issue of how location-based information and meta-data may be fed into “digital mass surveillance programs” engaged in by governments, which is beyond the scope of this commercially-oriented paper. In this regard, see United Nations, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism A/69/397 (23 September 2014) [footnotes omitted].

² Telstra, “Online Safety: Information about online privacy and tips on cyber-safety”, online: <https://www.telstra.com.au/privacy/online-safety>: “Smartphones have in-built features called geolocators that can give your exact location. Your whereabouts can be shared on social media or used by location services such as maps and public transport apps. Your position can also be embedded in images you take with your phone’s camera.”

³ Public Interest Advocacy Centre, “A Do Not Track List for Canada” (October 2009) online: <http://www.piac.ca/files/dnt_final_website.pdf>: “As mobile technology pushes ahead, location-specific behaviourally targeted marketing on mobile devices seems to be the next logical step for marketers.”

⁴ Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
devices increases.” In 2010 Industry Canada noted: “The possibility for, and likely business interest in, linking a consumer's location to a whole range of information about that consumer, has raised broad concerns.”6

As the European Union has noted:

Geographical information plays an important role in our society. Almost all human activities and decisions have a geographical component. In general, the value of information increases when it is connected to a location. All kinds of information can be connected to a geographic location, such as financial data, health data and other consumer behavioural data. With the rapid technological development and wide uptake of smart mobile devices, a whole new category of location based services is developing.7

Marketers are indeed keenly aware of how knowledge of a person’s location at a given time, and over time, can reveal details about an individual’s life. The traditional saying in real estate about the “three rules” being “location, location, and location” now also applies to a growing group of businesses attempting to capitalize on information about existing and prospective customers’ location. These businesses gain insight into consumers by inferring behavioural characteristics from places visited, daily travels and daily routines. This data can subsequently be cross-referenced with other data available to businesses, such as online browsing activity, purchasing history, and social media interactions.

The commercial appeal of location-based profiling is strong. According to one consultancy, “Digital and mobile delivery platforms enable brands to deliver messages and engage with their consumers at a level of intimacy never achievable before. … LBM [location-based marketing] offers the ability to understand customer profiles, behaviours, and purchasing habits well beyond traditional measurement of marketing and advertising spending. And we are not just talking about smartphones and tablets.”8 As one author for CSO Online (a publication for security and risk management professionals) reported:

It knows when you are sleeping. It knows when you're awake. And it's not Santa Claus. It is your increasingly smart smartphone, loaded with processors

5 OPC, Appearance before the Senate Standing Committee on Transport and Communications (December 8, 2009), online: <https://www.priv.gc.ca/parl/2009/parl_bg_20091208_e.asp>.
and apps that you acquired voluntarily, with "location services" that broadcast where you are and, in some cases, what you are doing.9

At a 2013 online advertising workshop, the Location-Based Marketing Association, an industry association, alluding to the prevalence and importance of browser “cookies” to online marketing, noted that “85% of data has a location element to it,” and that “location is the new [browser] cookie.”10

Indeed, the scale and scope of the business opportunities associated with so-called location-based marketing and location-based services (collectively, location-based technologies) have been well-documented in business literature. The opportunities for businesses to gain even more insights into consumer behaviour based on consumers’ whereabouts are said to be unprecedented given:

(i) the rapid growth in adoption and use by Canadians of smartphones and other mobile computing or “smart” devices with embedded GPS chips, such as tablets;
(ii) the rapid growth in adoption by businesses of RFID technology; and,
(iii) the increasing incorporation of location-based data into an increasing number of apps in use.

Growing privacy concerns

Are there privacy concerns about all of this collection, use and sharing of location information? Are Canadians sufficiently informed of these practices? As PIAC noted in its 2009 report, “it is unreasonable to expect consumers to complain about the practice when they are unaware of the extent to which their personal information is collected, used and disclosed for the purpose of online behavioural targeted advertising.”11

With knowledge about a person’s movements and movement habits, and location at a specific time, businesses, governments, criminals and others can infer detailed behavioural insights about a person. These entities may also be able to identify individuals despite their location information being stripped of any seemingly revealing information through processes such as anonymization and aggregation.

11 Public Interest Advocacy Centre, “A Do Not Track List for Canada” (October 2009), online: <http://www.piac.ca/files/dntl_final_website.pdf> at 76.
Smartphone users are likely not surprised that requesting directions via an app on their phone uses their location information to navigate. Such users are also likely not surprised that a wireless service provider’s network must be able to locate wireless handsets in order to provide voice and data services. However, smartphone users may be very surprised to learn that their location may be monitored by other apps not explicitly based on the use of location information. For example, the highly popular “Angry Birds” app collects users’ location information.12

As one author observed, “Almost every app gathers some kind of information,” but “connecting that data to the ostensible function of the app can be murky.”13 In 2013, for example, the United States Federal Trade Commission (FTC) censured the developer of a free flashlight app for collecting users’ location information without informed consent.14 To this day, the “permissions” sought by the app provider are extensive.15

---

12 See Angry Birds developer Rovio’s Privacy Policy (October 2013), online: <http://www.rovio.com/Privacy>

To the extent Rovio makes location enabled Services available and you use such Services, Rovio may collect and process your location data to provide location related Services and advertisements. For example, some add-ons or offers may be available at dedicated locations. The location data is processed and stored only for the duration that is required for the provision of the location related Services.

Rovio may use, depending on the service (1) IP-based location based on the IP address presented by the end-user, (2) fine geo-location data based on coordinates obtained from a mobile device’s GPS radio, or (3) coarse, network-based geo-location data based on proximity of network towers or the location of WiFi networks.

Your fine, GPS-based geo-location is not accessed without your consent. Notwithstanding Rovio’s partners who are providing location related parts of the Service, Rovio will not share your GPS geo-location with third parties without your consent. To the extent Rovio makes available GPS geo-location to third parties in accordance with this Privacy Policy, it will be provided anonymously.


14 Federal Trade Commission, Press Release, “Android Flashlight App Developer Settles FTC Charges It Deceived Consumers - ‘Brightest Flashlight’ App Shared Users’ Location, Device ID Without Consumers’ Knowledge” (5 December 2013). See also: Cecilia Kang, “Flashlight app kept users in the dark about sharing location data; FTC”, The Washington Post (5 December 2013), online: <http://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-rtc/2013/12/05/1be26fa6-5dc7-11e3-be07-00c6776266ed_story.html>; Robert McMillan, “The Hidden Privacy Threat of… Flashlight Apps?”, Wired (20 October 2014), online: <http://www.wired.com/2014/10/iphone-apps/>: “Even a flashlight app, it turns out, can ask for a shocking amount of user data when you download it, tapping everything from my calendar to my phone’s location engine to my camera. Yes, my camera. This is something you can keep in check, thanks to the privacy controls on today’s iPhone, but the truth is that most people don’t.”

15 Brightest Flashlight Free Version 2.4.2, the latest version available in the Google Play Store as of March 2015, requires the following permissions (see permissions list online: <https://play.google.com/store/apps/details?id=goldenshoretechnologies.brightestflashlight.free&hl=en>):

- **Location**: approximate location (network-based), precise location (GPS and network-based);
- **Photos/Media/Files**: modify or delete the contents of your USB storage, read the contents of your USB storage;
- **Camera**: take pictures and videos;
- **Wi-Fi connection information**: view Wi-Fi connections;
- **Device ID & call information**: read phone status and identity;
- **Other**: disable or modify status bar, read Home settings and shortcuts, control flashlight, prevent device from sleeping, view network connections, full network access, install shortcuts, uninstall shortcuts.
In 2014 the OPC, the “advocate for the privacy rights of Canadians,” noted that the developer of a similar type of free flashlight app sought a similarly broad set of permissions, such as access to the user’s camera/microphone, device ID, call information and even photos, media and other files. The developer did not make clear why the app would need “all that information to operate a flashlight,” and there was no “clear and accessible policy outlining how [users’] personal information would be used.”

App developers are not the only businesses collecting this type of information. At least one major Canadian wireless service provider has plans to re-activate a behavioural marketing program which uses information about its subscribers’ browsing activity and demographic information, including location, to behaviourally profile and categorize its customers and serve them targeted advertisements. This is described later, in the case studies section of “Chapter 2 – Location-based technologies: an overview.”

The collection and use of location-based information from mobile devices has caught the attention of privacy regulators in a number of jurisdictions within Canada. Federally, the OPC has frequently expressed concern about the extent of data collection, and the extent to which Canadians were being informed of it.

In 2012 the privacy commissioners of Canada, Alberta and British Columbia observed, “The mobile environment, along with the new app economy it has generated, is a rapidly evolving...”

---

16 Office of the Privacy Commissioner of Canada, “About the Office of the Privacy Commissioner” (5 December 2012), online: <https://www.priv.gc.ca/au-ans/index_e.asp>.


18 In response to a question from the CRTC to reconcile an example given about number of wireless subscribers active along a parade route, Bell stated that “in future we intend to aggregate information such as number of users on cell towers to approximate information such as foot traffic and busy times, which could assist other companies in understanding (for example) when to have additional staff on hand.” Part 1 Application CRTC 2014-0076-2, Application regarding Bell’s use of customer information (31 January 2014), online: <https://services.crtc.gc.ca/pub/instances-proceedings/Default-Default.aspx?Lang=eng6&YA=2014&S=C&PA=t&PT=pt1&PST=a>.

19 Office of the Privacy Commissioner of Canada, “Global privacy sweep raises concerns about mobile apps” (10 September 2014), online: <https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp>: “Fortunately, there were few examples of apps collecting the sort of information that would appear to exceed their functionality—like a flashlight app seeking permission to obtain your contacts list,” says Daniel Therrien, Privacy Commissioner of Canada. “But we did find many apps were requesting permission to access potentially sensitive information, like your location or access to your camera functions, without necessarily explaining why. This left many of our sweepers with a real sense of unease.” See also the discussion of PixelGun’s Terms of Use in Office of the Privacy Commissioner of Canada Blog, “From APP-laudable to dis-APP-ointing, global mobile app privacy sweep yields mixed results” (9 September 2014), online: <http://blog.priv.gc.ca/index.php/2014/09/09/from-app-laudable-to-dis-app-ointing-global-mobile-app-privacy-sweep-yields-mixed-results>: “[T]he terms of use policy [is] long and legalistic, an oft-cited complaint during last year’s sweep that’s particularly challenging on the small-screen.”
new frontier. As with past frontiers, it is filled with both richness and potential, but also risks.\textsuperscript{20}

The three privacy commissioners further stated:

> While the smart phone era brings unparalleled consumer connectivity and convenience, it also holds the potential for comprehensive surveillance of individuals. The novel uses of device sensors in apps, such as those that permit location awareness, provide the potential to follow where we go and, when combined with data on what we do and what we think, ultimately, to create a portrait of who we are.\textsuperscript{21}

In the same report, however, those privacy commissioners asserted that “Canada’s privacy laws require all businesses to balance innovation and entrepreneurialism with effective privacy protection.”\textsuperscript{22} From a consumer perspective, is that the case? As The Economist has noted: “Regulators [of privacy] around the world increasingly find that technology has outrun them and are trying to catch up.”\textsuperscript{23}

**The issue: Do the current privacy rules adequately address location?**

Thus, the central research questions this report aims to address are:

> Does the current legal and regulatory regime, which draws on elements of privacy law and telecommunications law, reflect broader social norms in respect of privacy? Do the legal, regulatory and self-regulatory approaches sufficiently protect consumers from the improper over-collection, misuse and inappropriate disclosure of their location-based personal information collected through mobile computing devices?

**Methodology**

In addressing the research question, this report draws on a literature review, comparative analysis of other jurisdictions, and a national telephone survey of consumer attitudes. In addition, the author reached out to an extensive list of representatives from industry academia and civil society for the purposes of consulting on their views. Of the approximately 80 invitees, approximately seven agreed to participate in that consultation, including one of Canada’s largest telecommunications service providers, the OPC, and one provincial Information and Privacy Commissioner. In January and February of 2015 the author conducted those consultations.


\textsuperscript{21} Office of the Privacy Commissioner of Canada et al, \textit{ibid}.

\textsuperscript{22} Office of the Privacy Commissioner of Canada et al, \textit{ibid}.

This methodology has been reviewed by a methodologist.24

Why is this important?

Canadians are increasingly concerned about privacy, as explained in “
Chapter 3 – Privacy concerns and consumer attitudes towards location-based technologies,” with use of their location being a predominant concern. Yet the literature on location-based information privacy and the media’s focus tends to be mostly commercially-oriented, i.e., addressing how to capitalize on the business opportunities.25 Little recent work from a consumer perspective has been undertaken to assess how current examples of location-based technologies fit within Canada’s current legal and regulatory framework.

The report also aims to serve as a useful compendium of relevant laws, regulations and policies in respect of location-based data, and recommend any changes necessary to bring location-based technologies within the appropriate legal framework.

Report structure

The remainder of this report is organized as follows. Chapter 2 defines and explains what location-based technologies are and why they are increasingly valuable tools for businesses, and gives examples of their use in Canada. Chapter 3 discusses the privacy risks associated with location-based technologies, including broader social concerns and specific examples of harm.

Chapters 4 and 5 review and assess the three main types of privacy protections available to users of technology. Legal privacy protections are reviewed in Chapter 4, and technological privacy protections and self-regulatory and voluntary approaches are addressed in Chapter 5. Chapter 6 address this report’s central question, and makes recommendations about possible legislative reforms based on the foregoing. Throughout this report references are made, where appropriate, to the views of stakeholders who participated in consultations with the author.

Chapter 2 – Location-based technologies: an overview

This chapter defines and explains what location-based technologies are and why they are big business, gives examples of their use in Canada, and describes Canadians’ views about the collection and use of information about their location.

What is location?

Most simply, “location” can be defined as information about a person’s physical presence in space. Location can have varying levels of precision: from exact (i.e., down to the exact geographical location), to general, providing information about a person’s physical presence within a certain area of space (e.g., within a city, a postal code, a neighbourhood, a shopping mall, a store, etc.). Location may be absolute (i.e., at a specific grid reference) or relative (e.g., “within 50 metres” of a specific place or other persons or types of persons).

Location may or may not be linked to a person’s physical presence in space in time – past, present, and, using predictive analytics, even in the future. For example, a person’s location can be expressed as “visited this store four times in the past 2 weeks,” “regularly transits the

---


Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

Location information or “location data” as it is called in the British legislation, is defined as “any data processed in an electronic communications network which indicates the geographical position of the terminal equipment of a user.” (The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, S. 2(1))


Off the Grid? Pinpointing Location-Based Technologies and the Law
Highway 401 from Whitby to Oshawa in the morning, and from Oshawa to Whitby in the evening, Monday to Friday,” or “spends 40% of their time in postal code M5C.” Predictively, based on information about a person’s habits, it may even be possible to anticipate where a person may be in the future.

Location may be two-dimensional – as in location according to latitude and longitude (“x” and “y” coordinates), and it may be three-dimensional, depicting latitude, longitude, and altitude (the “z” coordinate). For example, a person may be at a given address, such as 123 Main Street, or more specifically, 123 Main Street, 11th floor.

As Bennett et al. note, absolute location information is “immediately helpful in watching or finding people.”28 But the secondary uses of location information are what are said to be perhaps even more powerful. As Bennett et al. note, “Physical places, however, have their own meanings.”29 They identify three categories of secondary uses for location information: (i) “georelational,” (ii) “geosocial,” and (iii) “geoinformational.”30 “Georelational’ … has to do with the ability to place others on the same map as you.” “Geosocial’ … involves mapping personal position onto socially significant sites.”31 That includes information and inferences about a person’s location (examples given include home or work), at a given time (day or evening) and how different permutations of such information may have different meanings to the user of the information, such as how being at home during the day may have a different meaning than being home in the evening.32

What are Location-based Technologies?

A 2010 Consumer Trends Update from Industry Canada’s Office of Consumer Affairs defined location-based services as follows:

> Location-based services (LBS) use location information (from cellular networks, a phone’s global positioning system (GPS), or Bluetooth technology) to offer personalized marketing or services to users.33

Prior research has defined location-based technologies and location-based services as follows:

> Although we make reference to other kinds of tracking devices and systems, our primary focus is with technologies that meet three specific criteria. They must pinpoint locations; they must do so continuously, and they must do so in real time. So while RFID and Wi-Fi present related issues, only those services that can give coordinates by calculating the longitude and latitude of a

---

28 New Transparency Project, *ibid*.
29 New Transparency Project, *ibid*.
30 New Transparency Project, *ibid*.
31 New Transparency Project, *ibid*.
32 New Transparency Project, *ibid*.
person’s position are the ones considered location technologies in the sense used here. They can point to the exact place where the person is, and communicate this in real time to other persons or agencies, on an ongoing uninterrupted basis.”

"Location-based Services (LBS) are a relatively new generation of tracking devices and their applications.”

"This surveillance potential requires a further convergence of technology, standards-setting and organizational interests to produce what has come to be called, “location-based services” (LBS). … The combination of cellular technologies, geographic positioning systems (GPS) and mapping products has produced a number of new applications designed to assist consumers, employers, parents and others “locate” individuals and objects in real time.”

Due to the rapid pace of technological development, it is a challenge to precisely define the terms “location-based services” and “location-based technologies.” Nevertheless, for the purposes of this report, with its emphasis on business-to-consumer relationships, this report blends the foregoing definitions as follows:

**Location-based services use location-based hardware and software technologies to provide knowledge about a mobile device user’s absolute (exact) and relational location, in real time and over time, for the purpose of providing a service for which the user’s exact location is relevant, or for the purpose of providing personalized marketing services to the user, with or without the user’s knowledge or consent.**

Applications and businesses that make use of location-based technologies include:

- customer profiling and recommendation services;
- mapping and navigation services (e.g., Google Maps);
- alerting services (e.g., Rogers Alerts, which serves promotions on users’ smartphones based on a given location);
- human or asset resource tracking (e.g., Geoforce, which tracks ‘field asset’ locations through time);
- public safety alerting systems (in trial in a number of jurisdictions).

---


35 Lyon Report at 63-64 [emphasis added], ibid.


37 See e.g. in Canada “Public Safety Canada has requested that the CRTC Interconnection Steering Committee (CISC) initiate a new task to assist in the development of the technical specifications and network design of a wireless public alerting service for Canada” Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014-447 and 2014-448, Amendments to
• fitness trackers, used to monitor activity levels, distances walked or run, flights of stairs
climbed, etc. (e.g., Fitbit,38 Garmin39); and
• trend analysis (e.g., for transit,40 public health, or retail floor traffic).

Location is also “central to many if not most Connected Car applications.”41 “Connected cars”
are “vehicles that use wireless communications to send data from the vehicle to external
computers and/or service providers.”42 Connected car applications are outside the scope of this
report.43

Stakeholders in the location-based ecosystem include:

• consumers;
• device manufacturers;
• radio equipment manufacturers;
• telecommunications service providers (notably wireless service providers);
• advertising platforms;
• advertisers and advertiser networks; and
• regulators with responsibility for privacy rights (provincial and federal privacy
commissioners, Canadian Radio-television and Telecommunications Commission
(CRTC)).

---

40 See: Andrew Tillin, “Will Our Fitness Data Be Used Against Us?” (5 March 2015), Outside, online:
41 BC Freedom of Information and Privacy Association, “The Connected Car: Who is in the driver’s seat?” (24
March 2015), online: <https://fipa.bc.ca/wordpress/wp-content/uploads/2015/03/CC_report_lite.pdf>[
"Connected Car"].
42 “Connected Car”, ibid at 64:

In addition to vehicle monitoring and other location-related services noted above, GPS functionality in
Connected Cars allows for destination-finding services, real-time traffic and weather information,
estimated commute times, fuel station location and pricing, and parking services that guide drivers to
the closest available parking space.”

In the authors view, “The breadth and depth of information that can be culled from Connected Cars is
significant and goes beyond the data already available to mobile device operating systems and
mobile network providers.

43 See “Connected Car”, ibid for a thorough discussion of the issues surrounding connected car applications.
Why is location information collected?

This section explains the principal purposes for which location information is collected. In short, there are technical reasons, public safety reasons, and commercial reasons, with the latter eclipsing the former two.

**Technical reasons for collecting location information**

As a technical matter, location information is necessary for a telecommunications company to provide mobile services. Obviously, in order to connect a call or transmit data, a mobile network necessarily must “know” where its subscribers’ handsets are at any given point.

In the words of Rogers, the only telecommunications service provider that agreed to be interviewed for this report, “the [wireless] system by definition has to know where [subscribers] are, using home location register. Rogers, in that sense, is tracking you at all times. None of that is recorded, or even used, for any purpose, unless you make a phone call, which is logged as a transaction in the system. Otherwise, we don’t know where you are.”

This seems to contrast with the views of Professor Michael Geist, who indicated in the stakeholder consultation his belief that Canadian wireless service providers may actually be using location for more than simply service delivery.

What’s often happening now with wireless service providers isn’t quite a bait and switch, but a rather a blurring of the distinction between location tracking and how carriers acquire network usage information. The approach enables wireless service provider to maintain that they don’t use location info, but still effectively run behavioural marketing by purchasing the same information back from app providers.

For example, I was told there are a handful of widely used apps that cover the majority of smartphone subscribers. The wireless service providers are skating a very fine line – somebody else collects the geographic information running on their network and they buy it back. From perspective of end-user, that’s likely a distinction without a difference.

Whether or not telecommunications companies are using location information for more than technical reasons remains to be seen.

**Public safety reasons for collecting location information**

In addition to the technical need, location tracking has its origins in meeting public safety needs.

Traditionally, location information has been gathered for law enforcement and emergency services, and much of the current location tracking capacity of mobile service providers can be traced back to demands by regulators to improve the ability of first responders (police, fire and paramedics) to accurately locate emergency scenes. Beginning in 1996, the U.S. Federal
Communications Commission (FCC) adopted a series of rules to improve the quality and reliability of 911 services for wireless phone users, such as requiring all mobile devices that carriers sell to have location identification capabilities by 31 December 2002. These rules require providers to supply the location of a mobile device’s location “generally to within 50 to 300 meters, depending on the type of technology used.”

In Canada, the CRTC ordered all wireless carriers to implement the first phase of Enhanced-911 capabilities in 2003 and the second phase in 2009. The first phase required only the location of the cell tower that a caller was using during the 911 call, whereas the second phase required carriers to provide location information by GPS, or triangulation methods if the mobile device is not GPS-capable. In 2014, the CRTC made the goal of increasing wireless location accuracy for use in emergency calls a high priority. One of the ongoing challenges facing first responders, as identified in a special report to the Commission, is the provision of location information, and accurate location information, from mobile devices and IP-enabled devices which use geographically independent (as opposed to fixed) IP addresses.

When the first phase of Enhanced-911 capabilities were implemented, wireless carriers in the United States and Canada began to offer “finder” services to recoup the cost of investment. These services would use the mobile device’s location to provide a user with information of nearby services. For example, in 2002 Canadian carrier Bell Mobility launched the MyFinder service which offered directions to nearby restaurants, hospitals, automatic banking machines and gas stations based on the mobile device’s location. However, due to the inaccuracy of the location information provided to the user, such finder services failed to gain popularity.

**Commercial reasons for collecting location information**

Beyond the technical needs of mobile service providers and public safety entities, there is a distinctly commercial reason underpinning the collection and use of location information.

---

50  Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 104.
52  Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 104.
On the one hand, there is the tracking of objects (vehicles and goods) for the purposes of optimized (more efficient) supply chain management, as well as infrastructure management. Mayer-Schönberger and Cukier give the example of how UPS, a delivery service, uses location information in multiple ways, with results including reducing mileage by 30 million miles, saving 3 million gallons of fuel from being burned, and therefore 30,000 metric tonnes of carbon-dioxide from being emitted into the atmosphere. They give other examples of how such data can be used to create value (economic or social) in combination with other collected data, in order to make transportation system improvements, and more profoundly, life-saving inferences and predictions. But what Mayer-Schönberger and Cukier observe, and what this report is focussed on, is that “datafied location across time is most notably being applied to people” by wireless operators and third party apps which may even gather location information regardless of whether the app has a location-based feature, all in pursuit of building predictive models of individuals’ behaviour, including the use of other data sets (recombinant data) to better market to them. Furthermore, there may be “terrible consequences” to the collection and processing of “huge amounts of data from mobile phones to make inferences and predictions about human behavior.”

The scale and scope of the business opportunities associated with location-based technologies have been well-documented in business literature. The opportunities for businesses to gain even more insights into consumer behaviour based on consumers’ whereabouts are said to be unprecedented given:

(i) the rapid growth in adoption and use by Canadians of smartphones and other mobile computing or “smart” devices with embedded GPS chips, such as tablets;
(ii) the rapid growth in adoption by businesses of RFID technology; and
(iii) the increasing incorporation of location-based data into an increasing number of apps in use.

As Mayer-Schönberger and Cukier note in their book Big Data, the narrow technical use of location data by mobile service providers is giving way to opportunities to monetize that information. Some firms, thanks to their position in the information value chain, may be able to collect huge amounts of data, even though they have little immediate need for it or aren’t adept at reusing it. For instance, mobile phone operators collect information on their subscribers’ locations so they can route calls. For these companies, this data has only narrow technical uses. But it becomes more valuable when it is re-used by companies that distribute personalized, location-based advertising and promotions. Sometimes the value comes not from individual data points but from what they reveal in the aggregate. ...

53 Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A revolution that will transform how we live, work and think (Houghton Mifflin Harcourt: 2013) at 88-89.
54 Mayer-Schönberger & Cukier, ibid at 90-91.
55 Mayer-Schönberger & Cukier, ibid at 90 and 107.
56 Mayer-Schönberger & Cukier, ibid at 90-91.
57 Mayer-Schönberger & Cukier, ibid at 106-07 [emphasis added].
Even the most banal information may have special value, if applied in the right way. Look again at mobile phone operators: they have records of where and when the phones connect to base stations, including at what signal strength. Operators have long used that data to fine-tune the performance of their networks, deciding where to add or upgrade infrastructure. But the data has many other potential uses. Handset manufacturers could use it to learn what influences signal strength, for example, to improve the reception quality of their gadgets. Mobile operators have long been loath to monetize that information for fear of running afoul of privacy regulations. But they are starting to soften their stance as their financial fortunes flounder and they regard their data as a potential source of income. In 2012 the large Spanish and international operator Telefonica went so far as to create a separate company, called Telefonica Digital Insights, to sell anonymous and aggregated subscriber-location data to retailers and others.

In the case of Bell and its “Relevant Ads” program, described below, the mobile service provider itself is getting directly involved in the business of distributing personalized, potentially location-based advertising and promotions.

As Professor Rettberg notes, “You can easily see some of the consequences of your data being tracked.” But although one may see some of the consequences of their data being tracked, for example in what is reflected back to them on their social media pages based on their previous internet searches or self-identified statuses (e.g., single, married) and interests, there is a mushrooming “big data” industry developing and operating behind the scenes.

This boom in the location-based service industry is a significant addition to the “big data” analytics industry. In essence, those in the big data analytics industry purchases customer information from a wide range of sources, including banks, websites, and retailers. They then aggregate it, package it, and sell it to third parties for further retail purposes, or other purposes such as identify verification and background checks.

The “big data” phenomenon has been thoroughly explored by Viktor Mayer-Schönberger and Kenneth Cukier, who, like a number of other authors, argue that the nature of surveillance has changed.

As the use of mobile devices continues to grow in Canada, so does the volume of information being collected about users. One of the more prolific sources of mobile device user information

---

58 Jill Walker Rettberg, Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves (Palgrave McMillan: 2014) at 85.
60 See e.g. Jill Walker Rettberg, Seeing ourselves through technology: how we use selfies, blogs and wearable devices to see and shape ourselves (Palgrave McMillan: 2014) at 85.
has been, simply, the location of the device. The location information that mobile devices can generate and store can be both intimate and accurate, without the location information itself having to necessarily be precise.\footnote{For example, in 2011 German politician Malte Spitz sued German telecom operator T-Mobile to obtain the location metadata it held as a result of Spitz’s cellphone use, between August 2009 and February 2010. Spitz then gave that information to journalists at Zeit Online, who combined it with other publicly available information such as tweets and blog posts to paint an intimate picture of Spitz’s life during those 6 months. See Zeit Online, “Tell-all telephone” (26 March 2011), online: <http://www.zeit.de/datenschutz/malte-spitz-data-retention/>.}

As The Economist notes about mobile devices, “Being closely connected to people’s personal lives and daily habits, the mobile device is the true ‘mini-me.’ … From a commercial point of view, a mobile’s best feature is its location-tracking capability, which shows exactly where the phone is.”\footnote{The Economist, “Special Report: Advertising and Technology” (13 September 2014) at 7, online: <http://www.econ.ucla.edu/sboard/teaching/tech/economist_advertising_2014.pdf>.

How is location information collected?

Currently, there are multiple means by which a mobile device user’s location can be determined.\footnote{For one earlier description of the technologies see generally Eladio Martin et al, “Positioning Technologies in Location-Based Services” in Location-Based Services Handbook (CRC Press: 2010) at 33:}

Older mobile devices without built-in global position system (GPS) generally rely on fundamental geometric principles known as “signal analysis locating” that make use of the network’s infrastructure, while newer devices use GPS and device identification methods.\footnote{Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 102.}

In addition to the use of GPS in mobile devices, there is also the possibility of tracking the location of a device by way of its Media Access Control (MAC) address used for Wi-Fi or Bluetooth service.\footnote{Ann Cavoukian et al, “Building Privacy into Mobile Location Analytics (MLA) Through Privacy by Design” (March 2014), online: <https://www.ipc.on.ca/images/Resources/pbd-mla.pdf> at 2.}

In order to locate the positioning of mobile phones lacking GPS capabilities, a cellular network provider can use the signal a device transmits to nearby cell towers to infer the device’s location. This “network-based location analysis” is achieved by analyzing differences in the signal’s characteristics as received by multiple different cell towers, such as the signal’s strength, the time it took for the signal to arrive, or the angle at which the signal arrived relative...
to another tower.\textsuperscript{67} This analysis process is commonly called “triangulation,” though strictly, triangulation refers only to analysis using the angles between a mobile device and three cell towers.\textsuperscript{68} Network-based location analysis can be done with fewer or more than three cell towers, with accuracy increasing with the number of cell towers available.

A more common way to locate a mobile device is through the use of GPS, which allows service providers to accurately identify a mobile device’s location anywhere in the world. GPS works by measuring the difference between the time a signal was sent by a satellite and the time the signal was received by a mobile device. With at least three separate signals, a mobile device can calculate its position in latitude and longitude, accurate to within a maximum of 15 metres (depending on the quality of the received signal).\textsuperscript{69} Assisted-GPS, where some GPS data is provided by nearby cell towers, can be used to speed up location calculation or provide location information when a mobile device cannot receive a high-quality GPS signal.\textsuperscript{70}

Lastly, the newest method of location tracking takes advantage of the Wi-Fi and Bluetooth capabilities of modern mobile devices. Each Wi-Fi and Bluetooth chip in a mobile device is assigned a unique identifier called a MAC address, which is used to distinguish it from other devices communicating on the network. When Wi-Fi or Bluetooth is activated on a mobile device, the device periodically sends out a request to discover nearby Wi-Fi access points or Bluetooth devices.

A Wi-Fi or Bluetooth tracking system will sit by passively and listen for these requests, collecting each unique identifier and the signal strength of the request. Given the short distances at which Wi-Fi and Bluetooth operate, approximately 30-35 feet for Bluetooth and over 100 feet for Wi-Fi, these tracking systems can reliably infer the position and movement of individuals with mobile devices as they walk through a store or on the sidewalk nearby.\textsuperscript{71} Active Bluetooth beacon systems can have a range of over 200 feet.\textsuperscript{72}

\begin{thebibliography}{99}
\bibitem{68} Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 102.
\bibitem{69} Scassa & Sattler, \textit{ibid} at 103; “What is GPS?”, online: Garmin <http://www8.garmin.com/aboutGPS/>.
\bibitem{70} Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 103.
\bibitem{71} Ann Cavoukian et al, “Building Privacy into Mobile Location Analytics (MLA) Through Privacy by Design” (March 2014) at 2-3, online: <https://www.ipc.on.ca/images/Resources/pbd-mla.pdf>.
\end{thebibliography}
The following figure depicts a typical Wi-Fi tracking architecture:

![Wi-Fi tracking architecture diagram](image)

Figure 1. Example Architecture of a Wi-Fi tracking system

Location information is collected by organisations for a variety of purposes and uses, including intelligence, public safety, and commercial purposes. This report focuses on the use of location information for commercial purposes.

**Smartphone apps**

The next wave of location information services appeared in the form of apps that allowed consumers to “check-in” to their current location, or share their location with friends via social media. One of the more recognized social network services of this kind was Foursquare, a geosocial app that functions by sharing the location of individuals who download the Foursquare app and actively share his or her location.74

Following Foursquare’s lead, other social media services such as Facebook, Twitter, and Instagram have now added the option to share one’s location with friends or followers.75 These sharing capabilities have a variety of settings such as automatic location-posting, whereby each social media posting automatically includes location, or user-selected location-posting whereby the user must actively choose to publicly post location information.

For example, Twitter provides an automatic location-posting service that adds location-based information to each post (“tweet”) sent from a mobile device. This automatic feature is opt-in, and allows users to disable the automatic setting, or to de-select location for a given post.

---

73 Levent Demir et al, “Analysing the Privacy Policies of Wi-Fi Trackers” (March 2014), online: <https://hal.inria.fr/hal-00968585/document>.

74 Note that in mid-to-late 2014, Foursquare spun off this “check-in and social media” functionality into a separate app named Swarm. See “A look into the future of Foursquare, including a new app called Swarm” (1 May 2014), online: Foursquare <http://blog.foursquare.com/post/84422758243/a-look-into-the-future-of-foursquare-including-a>.

75 Kathryn Zickuhr, “Location-Based Services” at 4, online: Pew Research Centre <http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_Location-based%20services%202013.pdf>.
Twitter also allows users to identify publicly their location on a per-post basis. In both cases the user determines whether location information is publicly shared. The user can also click on a button to instruct Twitter to clear all of the user’s location information.

The Facebook app automatically can add location information about a poster, unless the user proactively deselects the location. Users have the option of making their location more specific by “checking in” to identifiable locations, such as a park or restaurant, or by adding a new location, and this specific location information will be added to each post a user submits.

Facebook users can also locate nearby businesses if those businesses have claimed a page for their business and provided location details, and locate nearby friends, although this feature does not appear to have been rolled out for all users. Any user with whom another user is “friends” can tag that user in a post with location-specific information in it, unless the user switches the default setting to one requiring the user to give permission for the tag to be public. Users cannot prevent being tagged by someone else in a post that includes location information; they can only prevent the tagged post from being visible on their own profile.

Location sharing apps are becoming increasingly popular, with many uses: from letting social network contacts know of one’s whereabouts, to obtaining location-based services such as driving directions from a mapping app or referrals for a type of service (e.g., restaurant or hotel) nearby, and to tracking movement for health and fitness.

Recently, “fitness trackers” and, laterally, fitness tracking apps for smartphones and smartwatches, have become very popular with consumers who have embraced self-measurement as a way to improve their lifestyles through tracking of various metrics, and notably movement. Metrics include such things as kilometres cycled or run, calories burned, steps taken, and flights of stairs climbed. One popular fitness tracker is Fitbit, and another is Apple’s “Health” app (which cannot be removed by users) for iPhones and iPads.

---

77 Facebook, “How do I change or remove my location when I update my status from my Facebook app?” (Accessed March 2015), online: Facebook <https://www.facebook.com/help/297024380340522>.
79 Facebook, “Can I block people from tagging me at a location?” (Accessed March 2015), online: <https://www.facebook.com/help/271045102906746>.
However, and as explained below, how app providers subsequently use the information collected by such devices and apps varies widely, and is often buried in difficult-to-read or difficult-to-understand privacy policies. In addition, Facebook itself is often used to authenticate other apps, which could mean that there is a further flow of information from the app to Facebook, or vice versa.

**Sensors**

Sensors are increasingly being used to track a wide range of information. Since the development of highly localized Wi-Fi and Bluetooth tracking systems, retailers have begun to use location information in sensor systems known as Mobile Location Analytics (MLA). Not only can these systems track a mobile device as it moves within the system’s range, but these systems can also analyze the habits of the owner of the mobile device, all without the explicit consent of the user.

MLA allows retailers and vendors to better understand consumers’ in-store behavior through generating reports of busy store areas, repeat visitors, sequential visits, wait times, and employee-to-customer ratios. Moreover, retailers now have the opportunity to optimize store layouts, merchandise carried, and scheduling and staffing. MLA can allow retailers to change their target audience and demographics, e.g., from younger males to older females. MLA can

---

81 For a review of the stated privacy policies and publicly available information about social networking services available to Canadians, see Canadian Access to Social Media Information Project, online: <http://www.catsmi.ca>. See also PrivacyGrade, provided by the Computer Human Interaction: Mobility Privacy Security Lab at Carnegie Mellon University, online: <http://www.PrivacyGrade.org>.

82 Ann Cavoukian et al, “Building Privacy into Mobile Location Analytics (MLA) Through Privacy by Design” (March 2014) at 3, online: <https://www.ipc.on.ca/images/Resources/pbd-mla.pdf>.
allow retailers to target specific patterns, *e.g.*, by offering more pastries as opposed to cookies, or by changing the length of time of promotions, depending on user behaviour.

While heavily popular with retailers and shopping centres, MLA is used by a wide range of organizations, events and for direct marketing purposes.

Libelium, for example, is a wireless sensor manufacturing company, focussing on creating mobile device detection devices for shopping and street activity, or vehicle traffic monitoring. Libelium’s device, the Meshlium Xtreme, detects all iPhones and Android devices that work with Wi-Fi or Bluetooth interfaces, with a detection rate of 95% of all devices. Their sensor systems are able to determine the MAC address of the wireless device, the distance of the device from the sensor, the manufacturer of the device, if the user is connected to Wi-Fi (and if so, the name of the Wi-Fi network), and the class of device (*i.e.*, smartphone, hands-free, computer). Libelium’s device, the Meshlium Xtreme, detects all iPhones and Android devices that work with Wi-Fi or Bluetooth interfaces, with a detection rate of 95% of all devices. Their sensor systems are able to determine the MAC address of the wireless device, the distance of the device from the sensor, the manufacturer of the device, if the user is connected to Wi-Fi (and if so, the name of the Wi-Fi network), and the class of device (*i.e.*, smartphone, hands-free, computer).83 The Meshlium Xtreme can be applied to determine the number of individuals passing daily on a street, how long people spend on a street, who is a local resident versus a visitor based on daily MAC address matches versus sporadic matches, and the routes that people take in shopping malls and the time they spend in each area.

Another MLA-based start-up company, Estimote Inc., focuses specifically on micro-location tracking using custom-designed Bluetooth beacons. In combination with a smartphone app, the first release of their system was able to accurately track the navigation of a person in a small space to within 1.5 metres of their actual position.84 Recent improvements allow the platform to...
track a user to within 4 metres in a 600 square-metre room. The system can track multiple users independently, with real-time access to their position, and can theoretically scale to any size room (e.g., airport or shopping mall).

Figure 4. Estimote Bluetooth beacon-based real-time position tracking system

While MLA in a retail setting is a popular use of location-based services, there are numerous applications in various industries such as healthcare, hospitality, logistics, and government. In addition, location-based services are also being employed in the transportation industry.

The Meshlium Xtreme can also be used for traffic and transportation purposes. The sensor can detect mobile devices found in vehicles even at speeds of 100km/h, monitor the average speed of cars with mobile devices in them, and monitor the number of cars passing a certain point of a road. This information can be used in conjunction to plan traffic prevention and determine alternative routes to take during traffic hours.

Similarly, Germany’s Mercedes-Benz and BMW are among automakers who have adopted location-based tracking instruments in their self-driving cars; these instruments are likened to

---

85 See comment by co-founder Jakub Krzych, online: <https://news.ycombinator.com/item?id=9503497>.
aircraft “black boxes.” There is a currently a debate in Germany on how personal driving data may be used and who should have access to it.88

Another way location-based services are being employed in the transportation industry is through parking. Canadian-based start-up HotSpot Parking, allows its customers to pay or top up their parking meters remotely through users’ mobile devices. While the service may be valuable to its customers, it is also potentially valuable for nearby businesses as it allows these businesses to advertise directly to customers of the service through the mobile device’s geolocation capabilities. HotSpot Parking has, for example, been able to track and determine how many customers have responded to these ads and those who have returned.89

Canadian companies currently publicly disclosing the use or trial of location-based technologies such as sensor systems include: Rogers Alerts,90 Bell’s “relevant advertising” program,91 CIBC’s “Bonus Rewards,”92 Hudson’s Bay,93 American Apparel,94 Cineplex Cinemas,95 Shoppers Drug Mart,96 Westjet97 and others. Other companies are promoting wearable technologies such as smartwatches and fitness trackers, which according to 2015 research by device manufacturer Ericsson AG, one-third of consumers either already have or want.98

---

91 Bell, “Relevant Advertising” (Accessed 5 February 2015), online: <http://www.bell.ca/Relevant-Advertising-program>: “Types of information that will be used” includes “[n]etwork usage information - such as app usage, location, web pages visited, TV viewing, calling patterns and other information associated with your network usage.”
92 CIBC, online: <www.cibcbonusrewards.com>. Users of this loyalty card can use a “mapping feature” to search for participating establishments near them on either their desktop or mobile device. When accessed via a mobile device the user is faced with a pop-up permission request window stating: “http://www.cibcbonusrewards.com” Would Like to Use Your Current Location”. Users then have the choice of “Don’t Allow” or “OK”. Users who select “Don’t Allow” may nevertheless enter addresses or cities or other location information to see participating establishments in the chosen area.
94 Ligaya, ibid.
96 Physicalytics, ibid.
97 Physicalytics, ibid.
Gaining increasing popularity, it has been forecasted that the location-based services market will grow from $8.12 billion in 2014 to $38.87 billion in 2019.  

Examples of location-based technologies

This section provides several examples of how location-based information is collected and used by commercial entities. It begins by examining the use of location-based information by Canadian telecommunications service providers (Rogers and Bell) and giving an example of a U.S. program (Verizon); it then provides an example of how one major mobile device manufacturer builds in location services into its devices (Apple), and then gives examples of how various companies use Wi-Fi “beacon” tracking services to collect and share location-based information (Turnstyle, Via, etc.).

Apple iOS location services

Apple Inc, the manufacturer of some of the world’s most popular smartphones (in addition to tablets and other ‘smart’ technology), has long dominated the global smartphone league tables, with various models of its iPhone mobile device ranking in several spots in the global “Top Ten” sales figures for 2014.

Apple’s iPhone device and “iOS” operating system software provide a range of location services. As Apple explains:

Location Services allows location-based apps and websites (including Maps, Camera, Safari, and other Apple and third-party apps) to use information from cellular, Wi-Fi, Global Positioning System (GPS) networks, and iBeacons to determine your approximate location.

Users control whether or not location services are enabled, and users “can individually control which apps and system services have access to Location Services data,” with the exception of emergencies in which case “location information may be used” regardless of the user’s choice to enable or disable location services.

According to Apple, “By enabling Location Services, location-based system services such as these will also be enabled:”

Popular Near Me: Your iPhone will periodically send locations of where you have purchased or used Apps in an anonymous and encrypted form to Apple to

---


improve a crowd-sourced database that may be used to offer geographically-relevant Apps.

Frequent Locations: Your iPhone will keep track of places you have recently been, as well as how often and when you visited them, in order to learn places that are significant to you. This data is kept solely on your device and won’t be sent to Apple without your consent. It will be used to provide you with personalized services, such as predictive traffic routing.

Location-Based iAds: Your iPhone will send your location to Apple in order to provide you with geographically relevant iAds. 101

Apple’s disclosure is illustrative and does not provide users with a full understanding of exactly how their location data is used. This lack of disclosure is an industry-wide problem not specific to Apple.

**Turnstyle Solutions**

Turnstyle Solutions is a Canadian company that uses MLA in determining consumer behaviour. After formally launching in 2013, by early 2014 Turnstyle grew to over 200 sensors across Toronto with over 3.5 million unique customer profiles in Canada. 102 Turnstyle offers two main types of location services: MLA and Social Wi-Fi.

To gather general analytic data, Turnstyle uses customized Wi-Fi base station sensors, each the size of a deck of cards, 103 that listen in as mobile devices broadcast their MAC addresses while looking for Wi-Fi hotspots. 104 The sensors do not require individuals to log onto a business’ Wi-Fi; as long as the mobile device has its Wi-Fi enabled, Turnstyle can gather data based on the device’s MAC address. Using sensors inside stores, retailers can “analyze overall foot traffic, window conversion, location of people within a store, repeat vs. first-time visits to a store, dwell times, and more.” 105

In 2014, Turnstyle mounted a high concentration of sensors in various businesses stretching a 1.9 kilometer radius on Toronto’s Queen Street West. 106 These sensors provide Turnstyle the capability of not only knowing which stores an individual has frequented, but also what they did or where they went on a particular day.

---

101 Apple, *ibid* [emphasis added].
102 Armina Ligaya, “‘It’s creepy’: Location based marketing is following you, whether you like it or not” (1 February 2014), *Financial Post*, online: <http://business.financialpost.com/fp-tech-desk/personal-tech/its-creepy-location-based-marketing-is-following-you-whether-you-like-it-or-not>.
106 Armina Ligaya, “‘It’s creepy’: Location based marketing is following you, whether you like it or not” (1 February 2014), *Financial Post*, online: <http://business.financialpost.com/fp-tech-desk/personal-tech/its-creepy-location-based-marketing-is-following-you-whether-you-like-it-or-not>.
For example, Toronto restaurant Happy Child used Turnstyle’s analytics to determine that 170 of its customers went clubbing a few months prior and that 250 customers went to the gym in that month. From this information, the owner of Happy Child started carrying workout tank-tops with the restaurant’s logo.\(^{107}\) Knowing these types of facts about customers can lead a business to offer a customized experience such as serving a specific type of food based on what restaurants their clients visit, or playing a particular type of music based on concerts attended.

As it stands, consumers are not made aware that a particular coffee shop, restaurant or retailer is using the MLA service; that information is not made public, unless the retailer chooses to explicitly inform its guests. This may lead to complicated privacy issues. When dealing with MLA, Turnstyle is imposing an implied consent model onto users, meaning they assume that users agree. The only way to prevent this type of information gathering is to either switch off Wi-Fi on a mobile device, or make an opt-out request to Turnstyle. Turnstyle is a member of the Future of Privacy Forum’s MLA Code of Conduct\(^{108}\) (discussed below) which requires participating companies to honour the requests of consumers who provide their MAC addresses to a central opt-out database.\(^{109}\)

---


Facebook account, a Twitter account, a cell phone number (verified through a text message), or an email address. The options available to users are at the discretion of the business.

![Figure 6. Example social Wi-Fi custom splash page](image)

If a user does not log in using his or her personal information, and if the business has decided to not provide a “guest” login\(^\text{110}\), they will not be permitted to browse the web.

By accepting the option to login through a social media account, users give their explicit consent for Turnstyle to use the provided information, unlike information gathering based on MLA services. For users who log in with their Facebook or Twitter account, this means providing Turnstyle with access to significant personal information available through those services, which is then aggregated and linked to the user's MAC address of their device:

---

\(^{110}\) See Turnstyle, “Turnstyle On-Site WiFi Terms of Service” (Accessed March 2015), online: <https://www.getturnstyle.com/legal/wifiterms>: section 2 notes “guest” access does not require providing additional information.
necessarily limited to: screen name, name, location, profile picture; and, other information which the OAuth procedure allows Turnstyle to access.111

Once the data is aggregated and analyzed, a relationship is built between the mobile device and the business. According to Turnstyle,

shoppers’ smartphones will automatically sign on to the WiFi going forward and you will be able to communicate directly with them via Push notifications. You will also be able to enable location and time sensitive campaigns personalized for each type of customer through your Turnstyle dashboard.112

While Turnstyle’s co-founder insists that the users’ identities remain anonymous, if an individual logs in to a Social Wi-Fi system using a social media account (e.g., Facebook or Twitter), Turnstyle can let businesses know the names or the handle names of those individuals from the linked account.113

While customers may know that they have logged in through Facebook in order to access the internet, they may be unaware that their consent meant that they gave Turnstyle full access to their personal information. As was the case with Turnstyle’s MLA service, the only way to opt-out is through the company’s opt-out tool. For users to fully understand the scope of information they are providing to Turnstyle, they would need to read three legal documents: the Privacy Policy; the Mobile Location Analytics Privacy Policy; and the Wi-Fi Terms of Service, totalling over 8,800 words.114 That is in addition to Facebook’s privacy policy and practices, the user’s individual privacy settings, and any privacy policies associated with the user’s mobile computing device.

Turnstyle’s privacy policy itself refers to “personally identifiable information,” a term and concept which the OPC has noted falls below the standard set by PIPEDA:

PIPEDA does not contain any definition for “personally identifiable information,” “non-identifying information” or “confidential information.” The term “personally identifiable information” is one that is used in other jurisdictions and typically refers to a narrow set of information that can be used to uniquely identify an individual. Examples include an individual’s name, address, national identification number or driver’s licence number. By

111  Turnstyle, ibid.
112  Quoted text is no longer available on Turnstyle’s “Social Wi-Fi” product page. See archived version available at Archive.org, online: <https://web.archive.org/web/20140209013227/http://getturnstyle.com/product/social-wifi>.
contrast, the concept of personal information as set out in PIPEDA has been interpreted by the courts and the OPC to apply more broadly.\textsuperscript{115}

The OPC, using PIPEDA’s standard of “personal information,” has taken a broader and more contextual approach to determining what information warrants privacy protections.\textsuperscript{116}

\textit{Via Informatics’s “LocationGenius”}

LocationGenius is a service provided by a Toronto-based marketing and analytics company called Via Informatics Incorporated (Via). LocationGenius uses cellular network and device data, mobile sensors, and social media data in order to generate customer profiles of people who use a mobile phone in the locations that the service covers.\textsuperscript{117} Via claims that the service is available for "just about any location in North America."\textsuperscript{118}

The primary source of data for LocationGenius is anonymous location data collected by mobile carriers.\textsuperscript{119} A mobile phone, whenever it is turned on, constantly emits "pings" in order to communicate with nearby cell towers.\textsuperscript{120} These communications between the mobile phone and the various nearby cell towers can be triangulated in order to determine the approximate location of the mobile phone.\textsuperscript{121} Via buys this data from mobile carriers, assigns each mobile phone a unique identifier, and is then able to build a profile of the mobile phone’s user based on the locations in which it is found throughout the day.\textsuperscript{122} For example, a mobile phone may be located at a particular place every night (indicating that its user lives there) and may make regular visits to particular retailers. Based on this type of location-based data, detailed profiles are built.

Via gathers similar data from other sources, such as small sensors that can detect Wi-Fi and Bluetooth-enabled devices and track them throughout the range of the sensor, which might cover, for example, a retail store.\textsuperscript{123} Via also gathers data from geo-stamped social media data.\textsuperscript{124}


\textsuperscript{116} Office of the Privacy Commissioner of Canada, \textit{ibid}.

\textsuperscript{117} LocationGenius, online: <www.locationgenius.com>.

\textsuperscript{118} LocationGenius, \textit{ibid}.


\textsuperscript{120} Tossell, \textit{ibid}.

\textsuperscript{121} Tossell, \textit{ibid}.

\textsuperscript{122} Tossell, \textit{ibid}.


\textsuperscript{124} Location Genius, online: <www.locationgenius.com>. 
These customer profiles are aggregated, and along with associated analytics, sold to businesses and public entities that want to know more about the customers that are found in their physical locales. All of the data is anonymous, without a name, phone number, or any other "Personally Identifiable Information" attached to it. According to Via, its "privacy architecture" prevents it "from ever accessing or delivering data that is considered Personally Identifiable Information for any users or devices." Critics, however, have suggested that de-anonymizing this kind of data is not overly difficult. Several mobile analytics companies have worked with a group called the Future of Privacy Forum in order to create a Mobile Location Analytics Code of Conduct to act as a self-regulatory mechanism for the industry, although Via does not appear to have signed the Code.

Via / LocationGenius did not appear to have a publicly available privacy policy.

**iBeacon technology**

With Apple’s release of iOS7 in the summer of 2013 came its iBeacon technology, a technology that is centered on location information and that is powered through low energy Bluetooth. There are two parts to iBeacon technology: the first being the actual iBeacon sensors that can sense iOS powered devices, while the second are mobile device apps that incorporate iBeacon technology to gain location information. According to Apple,

[y]our iOS device can alert apps when you approach or leave a location with an iBeacon. In addition to monitoring location, an app can estimate your proximity to an iBeacon (for example, a display or checkout counter in a retail store). Instead of using latitude and longitude to define the location, iBeacon uses a Bluetooth low energy signal, which iOS devices detect.

Unlike other sensors or beacons, in order to use iBeacon technology, a user must not only be connected to Bluetooth but must also download the business’ or venue’s app; otherwise a user’s mobile device will not be affected. Effectively, this model is likened to the user opting-in to disclosing their location information. However, once the app has been downloaded, the iBeacon system will continue to interact with a user’s mobile device even if the app is not currently running. For example, if a store’s app is off on a user’s device, but a user walks into the store which contains iBeacon sensors, the user will get a push notification or message sent to their

---

125 Madhumita Venkataramanan, "My identity for sale" (30 October 2014), Wired, online: <http://www.wired.co.uk/magazine/archive/2014/11/features/my-identity-for-sale>.
lock screen upon entering the store. If the notifications are of use to the user, this will lead to the user launching the app and participating.\footnote{128}

Another differentiating factor of iBeacons is that the sensors do not track or collect location information from a user’s mobile device. iBeacon sensors, as the system currently operates, only \emph{send} information to an iBeacon enabled app, in order for the app to transmit information to a user’s device via a popup message.\footnote{129} The user’s mobile device does not \emph{request} information, which would provide the sensor system with the device’s unique Bluetooth MAC address. Any additional collection of location information occurs through a mobile device’s Wi-Fi network or mobile broadband connection that is controlled entirely by the app. However, turning off Bluetooth, updating the location permissions on a mobile device, or simply uninstalling the app will remove a device out of any iBeacon system.\footnote{130}

\textbf{Swirl iBeacon app}

At present, iBeacon retail apps are beginning to emerge across the United States. American companies such as Swirl and ShopKick are using the iBeacon system to build their MLA technology that could soon make its way to Canadian retailers, vendors and organizers. Unlike Turnstyle, Via and many other MLA companies, the apps of these companies only work with the consent of the mobile device user through the use of iBeacon technology.

In the case of Swirl, American retailers such as Kenneth Cole, Timberland, and Alex and Ani advise their shoppers of the option of downloading Swirl’s location tracking app in exchange for discounts on full-priced merchandise.\footnote{131}

For example, the app may send push notifications to users of the Swirl app for specific discount offers, or the app may direct users to a specific area in the store based on past purchases.\footnote{132} The appeal of Swirl, at least according to its business customers, is that because Swirl is an “opt-in” service that requires explicit consent, consumers are more receptive to it.\footnote{133}

Whether that is true, however, remains to be seen, but it begs the question about whether consumers appreciate the full extent of what they are “opting in” to or the effect of any

\begin{footnotes}
\item[133] See Swirl, online: <http://www.swirl.com/why-swirl/>.
\end{footnotes}
subsequent “opting out.” This issue of the blurring line between opting in and opting out, in the mobile context, will be explored later in this report.

In 2014, Swirl commissioned an independent study revealing that women were willing to share personal information with retailers when given something in return. In fact, the better the deal, the more willing women were to share their information. In response to the results, Chief Executive Officer of Swirl Hilmi Ozguc stated:

Consumers aren't completely opposed to sharing their location information ..., but they do want to have control over that information and get a tangible benefit in return for sharing it.

The same rules apply in retail: if brands create value (like highly relevant, personalized offers and content) for in-store shoppers by using their location, then consumers would be much more willing to share that information. ¹³⁴

![Figure 7. Swirl Study Infographic](image)

There is, however, a caveat in using this service. In addition to the app’s in-store capabilities, the Swirl app will collect location information through a user’s mobile device, the device’s geolocation or its GPS. Furthermore, the aggregate of personal information may be collected by Swirl and its affiliates to conduct research to determine users’ demographics, interests and behaviours. Lastly, it appears that while individuals may be willing to exchange location information for something in return, users may not be aware that by downloading and opting-into

¹³⁴ Swirl commissioned independent research firm ResearchNow to study the apparel shopping behaviors and preferences of 1,000 smartphone-owning women shoppers from March 25-26, 2013. The margin of error was +/- 3 percent; see Swirl, “#Privacy and #Retail: Swirl Study Finds Half of Female Shoppers OK with Retail Tracking If There is a Value Exchange” (17 July 2013), online: <https://www.swirl.com/pr-07-17-13.html>.
Swirl’s app, they are allowing Swirl to make their personal information public. For example, if a user has logged onto the Swirl app through Facebook, their Facebook postings may be used or accessed by third parties.135

**Major League Baseball iBeacon app**

Although iBeacon technology has had its fair share of success in the retail industry, it is not limited to the retail context. In early 2014 Major League Baseball (MLB) installed the technology in the ballparks of 20 out of the 30 teams in the league.136

The app, “MLB.com Ballpark,”137 is said to allow MLB to improve on fan experience through various means such as precisely directing fans to their seats quickly and easily, or offering fans discounts on concessions. The application will also allow MLB to collect a mobile device’s location information inside the stadium, and monitor how many times a fan has visited a specific location. This in turn is supposed to allow MLB to create “micro-locations” within stadiums, where MLB can tailor different experiences for different fans.138

**Verizon Wireless Smart Rewards**

In July 2014, the largest American wireless service provider, Verizon Wireless,139 launched a mobile device rewards program called Smart Rewards.140 To join, customers opt-in through registration. Smart Rewards offers Verizon Wireless subscribers discounts on merchandise, local dining and travel accommodations using a points-based system. Points can be obtained in numerous ways: for simply being a Verizon customer, through upgrading a basic phone to a smartphone, connecting a tablet to an existing plan, visiting the Verizon website or app, using paperless billing, or paying a bill online.

---

137  See MLB, online: <http://mlb.mlb.com/mobile/ballpark>.
139  Largest by number of subscribers, see e.g. FierceWireless, “Grading the top 8 U.S. wireless carriers in the fourth quarter of 2014” (3 March 2015), online: <http://www.fiercewireless.com/special-reports/grading-top-us-wireless-carriers-fourth-quarter-2014>.
However, in order to sign up for Smart Rewards, customers are required to sign up to Verizon Selects, a company program that tracks and collects data on mobile users, including location information.\(^{141}\) According to Verizon Wireless:

Verizon Selects will use location, web browsing and mobile application usage data, as well as other information including customer demographic and interest data, to create specific insights. Verizon Selects analyzes this information about customers to see whether they fit into certain audiences Verizon or third party marketers are trying to reach. Depending on the results, participating customers will receive marketing messages or offers that may be of more interest to them than what they see or receive today. These messages could be delivered in various ways such as email, text, postal mail or online or mobile advertising.\(^{142}\)

Users can opt out of the Verizon Selects program after signing up for Smart Rewards, however any data collected will be kept for up to three years.\(^{143}\)

**Canadian telecommunications service providers**

While telecommunications service providers (TSPs) have traditionally possessed significant information about their customers, they have often struggled with how to extract value from the information due to lack of internal expertise.\(^{144}\) However, TSPs, who have arguably the most direct access to a mobile user’s location information, have recently introduced location-based services built on top of their mobile wireless services.

**Rogers Alerts and Rogers OutRank**

In October 2013, Rogers Communications Inc. introduced a location-based service named Rogers Alerts.\(^{145}\) The service allows advertisers and businesses to send a personalized text message to a subscriber’s mobile device when he or she passes by a participating retail location. A Rogers mobile wireless subscriber must opt-in to the program by signing up, after which Rogers will give the subscriber a one-time credit of $5 on their wireless bill.\(^{146}\) Rogers claims that subscribers will not receive more than five advertising messages per week,\(^{147}\) up

---


\(^{146}\) See Rogers, online: <https://rogersalerts.ca/sho/rogers/register.html>.

\(^{147}\) See Rogers, online: <https://rogersalerts.ca/sho/rogers/register.html>.
from four per week when the service first launched. When signing up, the customer can choose to customize their experience by tailoring their discounts to retailers such as Future Shop, Sears Canada, Pizza Hut, A & W and Second Cup.

Rogers Alerts is based on technology from American company Placecast, called ShopAlerts. Since the technology is run from within a wireless carrier’s network, subscribers do not need to have a GPS-capable smartphone, or have any other smartphone location services enabled to receive promotional messages. ShopAlerts appears to take advantage of the information available to mobile wireless network operators who, by virtue of a mobile wireless network’s architecture, are always aware of where a cellular device is within its network. A Placecast case study suggests that Rogers Alerts subscribers have been very receptive to the program. According to a Rogers executive interview for this report, the Roger system is programmed in a

---


150 See Rogers, online: <https://rogersalerts.ca/sho/rogers/register.html>.

151 See Placecast, online: <http://placecast.net/about.html>.

152 Very little information is available publicly on the technical details of Placecast’s ShopAlerts platform, however media reports note that the geofencing is “deployed by the carrier” and Placecast’s platform establishes a subscriber’s location “through a carrier’s network.” See Ryan Kim, “O2 Turns on Geo-fencing for Starbucks, L’Oreal in UK” (14 October 2010), online: Gigaom <https://gigaom.com/2010/10/14/o2-turns-on-geo-fencing-for-starbucks-loreal-in-uk/>.


---
way that geo-fences locations and then pushes messages to those subscribers in the opt-in database.

Rogers also offers its “OutRank” service to businesses. A recent report alleges that Rogers, in its capacity as one of Canada’s largest wireless service providers and internet service providers, is “definitely selling your location data. They are selling your location data even if you are not a Rogers customer.” It is not apparent, based on Rogers’ marketing materials for OutRank, if or how Rogers may be doing this. In the online marketing materials for OutRank, Rogers states that its “Max” service will, for example, “find the prospects from the areas you serve who haven’t found you yet, but are looking.” Using or tracking location would appear to contradict statements by a Rogers’ executive that they do not track location information.

Bell’s “Relevant Ads” Program

In October 2013, Bell Mobility Inc. (Bell) issued an “Important notice about how Bell uses information” to its subscribers, delivered by email, and also made available online. The notice described a new Bell marketing initiative involving the collection of personal information (including location-based data), customer profiling, and online behavioural marketing.

Recipients and viewers of the notice were informed that, starting on 16 November 2013, “Bell will use certain information” about their “account and network usage for select purposes.” The notice provided illustrations of the categories of information (network usage information, account information) and the types of information (e.g., browsing history, location, TV viewing, calling patterns, gender and age), that Bell would begin collecting. The notice also provided illustrations of how that information will be used, such as to “create better business and marketing reports,” for “other companies to create business and marketing reports,” and to “make ads you see more relevant.” Existing and new subscribers would automatically have their information fed into the advertising program, subject to an online opt-out mechanism.

In response to an unprecedented number of complaints, the OPC announced on 23 October 2013 that it would investigate Bell’s new advertising program. On 7 April 2015, the OPC released its report which found that Bell’s opt-out consent mechanism did not meet the standard of consent required under federal privacy law, given the sensitivity of information the system collected. In January of 2014 PIAC and the Consumers’ Association of Canada filed a complaint with the CRTC arguing that the behavioural marketing program is unlawful under

154 See Rogers, online: <https://www.rogersoutrank.com/>.
155 See Devonavar, “Is Rogers Selling your Location Data?”, online: <http://devonavar.ca/open-culture/privacy/is-rogers-selling-your-location-data/>.
156 Devonavar, ibid.
157 Office of the Privacy Commissioner of Canada, “Results of Commissioner Initiated Investigation into Bell’s Relevant Ads Program” (7 April 2015), online: <https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_e.asp>.
158 See Public Interest Advocacy Centre and the Consumers’ Association of Canada’s applications regarding Bell’s use of customer information, CRTC File #8665-P8-201400762 – Requests for Information, online: <https://services.crtc.gc.ca/pub/instances-proceedings/Default-Default.aspx?lang=eng&YA=2014&S=C&PA=t&PT=pt&PST=a#201400762>.
the *Telecommunications Act*.\(^\text{159}\) It is noteworthy that the OPC qualified their recognition of the Bell program as having an appropriate purpose as being subject to any CRTC decision.\(^\text{160}\)

The OPC’s findings included that:

- personal information it collects for the primary purpose of delivering telecommunications and broadcasting distribution services was now being used for the secondary purpose unrelated to the primary purpose: enabling third-party behaviourally-targeted advertising;\(^\text{161}\)
- many of the terms which Bell indicated it would be using for its behavioural marketing program, including “location,” were not explained in sufficient detail;\(^\text{162}\)
- Bell was using sensitive web-surfing information (URLs) to populate non-sensitive marketing categories;\(^\text{163}\)
- “the breadth of the information Bell retains for the RAP, including all URLs visited by the Bell Customer during the past 90 days, is more sensitive than the individual elements of that information”;\(^\text{164}\) and
- considering the “sensitivity of the information used by Bell ... in the aggregate ... Bell has access to vast amounts of information about its customers. ... Bell can use this information to infer a wide range of both general and specific interests. The combination of this information with the extensive account/demographic information (e.g., age range, gender, average revenue per user, preferred language and postal code) used by Bell for the RAP will result in highly detailed and rich multi-dimensional profiles that, in our view, individuals are likely to consider quite sensitive.”\(^\text{165}\)

Accordingly, the OPC determined that Bell customers would expect opt-in consent, and therefore the OPC recommended that Bell obtain consent for any future uses of other information, including that related to mobile location, and that Bell must be able “to provide a sufficiently clear and detailed explanation of intended uses to support meaningful consent.”\(^\text{166}\)

The OPC found that while mobile location information was not yet being used in the advertising program, the system did have the capability to track, collect and use mobile device location information. Bell has since stopped operating the advertising program and deleted the personal information it collected since its inception.
Originally, Bell had indicated that it would not adopt the OPC’s opt-in consent recommendation, and the OPC stated its intention to bring the matter to the Federal Court to force Bell to change its program, if Bell did not voluntarily do so.\textsuperscript{167} Bell subsequently indicated to the OPC that it was withdrawing its program, and that “if it launches a similar program in the future, it would do so using express opt-in consent.”\textsuperscript{168}

Whether or not the CRTC will declare, in response to a complaint\textsuperscript{169} by PIAC and the Consumers’ Association of Canada, that the program is unlawful under the \textit{Telecommunications Act}, remains to be seen. It is noteworthy that the OPC qualified their recognition of the Bell program as having an appropriate purpose as being subject to any CRTC decision, stating, “If it were determined that Bell cannot, pursuant to the \textit{Telecommunications Act}, legally engage in the RAP, this would be another factor which may impact on our s. 5(3) analysis.”\textsuperscript{170}

\begin{footnotes}
\item[167] Office of the Privacy Commissioner of Canada, \textit{ibid.}
\item[168] See Office of the Privacy Commissioner of Canada’s updated findings. See also Jeff Jedras, “Bell kills Relevant Ads Program over privacy concerns” (13 April 2015), \textit{IT Business}, online: <http://www.itbusiness.ca/news/bell-kills-relevant-ads-program-over-privacy-concerns/55041>.
\item[170] Office of the Privacy Commissioner of Canada, “Bell advertising program raises privacy concerns” (7 April 2015), online: <https://www.priv.gc.ca/media/nr-c/2015/nr-c_150407_e.asp> at para 56.
\end{footnotes}
Chapter 3 – Privacy concerns and consumer attitudes towards location-based technologies

This chapter describes the types of privacy risks that location-based technologies pose, and how consumers view those risks. First it surveys the major concerns expressed about the collection and use of location information. It describes broader social concerns, and gives specific examples of harm. Then, it aggregates past research and consumer surveys, and details the results of a PIAC-commissioned survey.

A report by the European Network and Information Security Agency documents several classes of risks and vulnerabilities that smartphone users face, including security vulnerabilities in smartphone software architecture, limited possibility for after-market security solutions, “user permission fatigue” which limits the usefulness of install-time permission requests, lack of privacy best practices and lack of user awareness.171 One pertinent weakness is that “[t]here is no means to set global policies for permissions granted, e.g., ‘do not install any apps which request location data for marketing purposes.’” But as it will be explained there are broader social risks involved in the collection and use of personal information, as well as specific risks to those who personal information is collected.

Risks and concerns with location-based information tracking

This section highlights some of the risks that have emerged from the growing use of location-based technologies, and highlights expressions of social concerns with, as well as specific examples of harm.

The dangers of collecting and analyzing fine-grained personal information such as location data have been the growing focus of a number of researchers.172

First and foremost, the more data-points about an individual that can be collected and assimilated into a profile about an individual, the more ways that individual can be influenced by whoever can view the data:

Even when people intentionally make their geolocation data available on the Internet, through whereabouts and geotagging services, the unlimited global access creates new risks ranging from data theft to burglary, to even physical aggression and stalking.


As with other new technology, a major risk with the use of location data is function creep, the fact that based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of the data.\textsuperscript{173}

Location data is also more revealing than people may believe. In isolation, a particular location data point may not mean much, however:

Combined or accumulated over time, such data … becomes highly revealing. It can divulge the identity of an otherwise unidentified person, as well as that person’s habits, routines and social circle. It can be used to ascertain the person’s religious and political associations. It can show when a person deviates from their normal routine, develops a health problem, or engages in activities that, if known, could harm their reputation.\textsuperscript{174}

In a special report on “big data” and the advertising industry, \textit{The Economist} notes that while even China has publicly stated its intention to increase data security and privacy for consumers, the United States (where most big data companies operate) shows little sign of increasing oversight of the industry:

According to Jim Halpert of DLA Piper, a law firm, who co-chairs its global data-security practice, “the issue is not advertising. It is rather that some entities can sell lots of information about individuals without those individuals knowing about it.” There is very little oversight of how this information is used or where it is sold. … So far concerns about unfair practices have been raised mainly by academics, tech geeks and some vigilante consumers, not the public in general, but that may be because most people do not even know they are being followed.\textsuperscript{175}

The OPC has itself recognized a broader concern with what it has referred to as the risk of personal information entering an “unchecked international market in personal information.”\textsuperscript{176}

\textbf{Social concerns with behavioural profiling}

The collection and use of personal information raises well-documented social concerns over what Professor David Lyon termed “social sorting.”\textsuperscript{177} Professor Lyon, noting that while this is

\textsuperscript{173} The European Union’s Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, \textit{Opinion 13/2011 on Geolocation services on smart mobile devices} (May 2011) at 7.


\textsuperscript{176} Office of the Privacy Commissioner of Canada, “Review of the regulatory measures associated with confidential customer information and privacy” (March 2009).


“Social sorting” highlights the classifying drive of contemporary surveillance. It also defuses some of the more supposedly sinister aspects of surveillance processes (it’s not a conspiracy of evil intentions or a relentless and inexorable process). Surveillance is always ambiguous (Lyon 1994: 219; Newburn
neither “a mere ‘technological’ phenomenon,” nor a “necessarily negative one, socially speaking,” framed the issue, as follows:

Codes, usually processed by computers, sort out transactions, interactions, visits, calls, and other activities; they are the invisible doors that permit access to or exclude from participation in a multitude of events, experiences, and processes. The resulting classifications are designed to influence and to manage populations and persons thus directly and indirectly affecting the choices and chances of data subjects. The gates and barriers that contain, channel, and sort populations and persons have become virtual.

Professor Lyon, via an extensive review of the literature explains how geodemographic information, combined with other information, and “phenetics” (classification based on measurable similarities and differences) can be used in harmful ways which challenge social justice. The upshot:

Groups likely to be valuable to marketers get special attention, special deals, and efficient after-sales service, while others, not among the creamed-off categories, must make do with less information, and inferior service. Web-based tools have broadened these processes to include other kinds of data, relating not only to geodemographics but to other indicators of worth as well. In processes known variously as “digital redlining” (Perri 6 2001) or “weblining” (Stepanek 2000), customers are classified according to their relative worth. So much for the sovereign consumer! The salesperson may now know not only where you live, but details such as your ethnic background (Stepanek notes that in the USA Axxiom matches names against demographic data to yield “B” for black, “J” for Jewish, “N” for Nipponese-Japanese and so on).

One example of social sorting is a practice known as “price steering”, through which retailers can use location information to offer higher or lower rates to people based on their location:

Travel websites and other Internet retailers may be giving your friend better deals than you as part of a high-tech experiment called price steering that gives consumers different search results based on their buying histories, tastes — even the types of digital devices they shop on. …

When users of GPS-enabled mobile devices search for lodging, Orbitz can detect their current locations and automatically steer them toward nearby hotels — something that is not possible for desktop users. 178

Location data can also be used against consumers in ways that many people might consider unfair or abusive. Professor Lori Andrews described the example of a businessman named Kevin Johnson, who discovered, after returning from his honeymoon, that the credit limit on his

and Hayman 2002: 167–8). At the same time social sorting places the matter firmly in the social and not just the individual realm – which “privacy” concerns all too often tend to do. Human life would be unthinkable without social and personal categorization, yet today surveillance not only rationalizes but also automates the process.

American Express card had been lowered from $10,800 to $3,800. In a letter, the company explained that “[o]ther customers who have used their card at establishments where you recently shopped have a poor repayment history with American Express.” With the location data provided by location-based technologies, this kind of discrimination is possible in a wide variety of circumstances. Professor Andrews notes the possibility, for example, of life insurance being denied to a consumer because location data indicates the individual frequenting fast food restaurants.

Location data can also be used in ways consumers may not have anticipated, such as in a lawsuit. A personal injury lawsuit was launched in 2014 that sought to use Fitbit activity level data to show a plaintiff is still below the typical activity level for someone her age, years after an injury. As one commentator noted:

> The case opens up the possibility that fitness trackers and other wearable computing devices could be used in future cases with a grander scope. Though the data is willingly being turned over by the plaintiff in this case, data from wearables could be subpoenaed by courts as evidence in more serious cases.

More broadly, Mayer-Schönberger and Cukier argue that there many other systemic risks associated with the unprecedented, surging gathering, storing and reusing of personal information. In their book *Big Data*, they argue that with the trend toward “big data, the value of information no longer resides solely in its primary purpose ... it is now in secondary uses,” made possible through the lowered cost of data, and mathematical ways to reuse it, combine it with other data, and to design “extensibility into it from the outset so that is it suitable for multiple uses,” including uses that may only be realized as possible in the future. As the size and scale of data collection increases over time, privacy will continue to be endangered even more, through penalties to people based on their “propensities” (judging people and punishing them before they have even acted), and become a source of further repression by the powerful. In their view:

> The stakes are higher than is typically acknowledged. The dangers of failing to govern big data in respect of privacy and prediction, or of being deluded about the data’s

---

180 Andrews, *ibid*.
181 Andrews, *ibid*.
183 Gibbs, *ibid*.
185 Mayer-Schönberger & Cukier, *ibid* at 104-12 and 153.
meaning, go far beyond trifles like targeted online ads. The history of the twentieth century is blood-soaked with situations in which data abetted ugly ends.\textsuperscript{186}

These concerns are echoed by a number of other academics, including several who participated in the stakeholder consultation for this report, as discussed below.

\textit{Examples of specific harm}

This section provides some specific examples of how location information can be used in harmful ways. Real harm may accrue in a number of different situations, whether relating to the discrete knowledge of an individual’s location, or to behavioural insights and inferences that may be gleaned from information about the individual’s habits. More systemically, there are concerns over the social impacts of behaviourally-based marketing.

\textit{Arias v. Intermex Wire Transfer, LLC}

One potential way that individuals can suffer harm as a result of location-based technologies is through being tracked by their employers.

In May 2015, a California woman claimed she was fired from her job at the money transfer firm Intermex after uninstalling an app on her smartphone used by her employer to track her movements 24 hours a day.\textsuperscript{187} In April, 2015, Myrna Arias and other employees of Intermex were asked to download an application called Xora StreetSmart to smart phones issued to them by their employer.\textsuperscript{188} Ms. Arias's employment as a sales executive consisted of travel throughout central California to persuade business owners to install the company's money transfer machines.\textsuperscript{189} Xora is a timecard smartphone application that tracks the exact location of the person who has the application installed on their wireless device.\textsuperscript{190} Intermex was allegedly tracking employees in order to monitor whether it needed to buy company cars.\textsuperscript{191}

When Ms. Arias voiced a concern the monitoring of her location during non-work hours was an invasion of her privacy, her supervisor at Intermex advised her to keep her smart phone on at all

\begin{footnotesize}
\begin{enumerate}
\item Mayer-Schönberger & Cukier, \textit{ibid} at 151.
\item James Vincent, “Woman fired after disabling work app that tracked her movements 24/7” (13 May 2015), The Verge, online: <http://www.theverge.com/2015/5/13/8597081/worker-gps-fired-myrna-arias-xora>.
\item Courtney Rae King, “Employee GPS Tracking: There’s an app for that, but does it come at a cost?” (19 May 2015), online: Ice Miller LLC <http://www.icemiller.com/ice-on-fire-insights/publications/employee-gps-tracking-there-s-an-app-for-that-but/#sthash.T2N5n5wQ.dpuf>.
\item Arias v Intermex Wire Transfer, LLC (5 May 2015), Cal Sup Ct, Complaint for Damages at 3, online: <http://cdn.arstechnica.net/wp-content/uploads/2015/05/Intermexcomplaint.pdf>.
\item Aimee Picci, “Do companies have a right to watch employees 24/7?” (14 May 2015) CBS, online: <http://www.cbsnews.com/news/do-companies-have-a-right-to-track-employees-247/>.
\end{enumerate}
\end{footnotesize}
times to answer phone calls from clients." In late April, Ms. Arias de-installed the application and on May 5, 2015, she was dismissed by Intermex. Ms. Arias is now suing Intermex for violating her privacy and wrongful termination, among other allegations.

**Domestic Abuse and Stalking**

There are a number of instances of location-based technologies being used in the context of domestic abuse and stalking. For example, in 2009, a Texas man allegedly used a location-tracking service offered by his cellular carrier to track his wife to a friend’s home to which she had fled. According to police, he subsequently assaulted her and took her car. The man reportedly acknowledged in an interview using the tracking service to track his wife, saying that "AT&T had this little deal where you could find your family member through her cellphone." A 2009 US Department of Justice report estimated that there were more than 25,000 instances of GPS stalking annually in the United States. While data for Canada is not available, the availability of similar technology and services means that the situation is likely to be similar. In addition, the report used data from 2006, before the popular iPhone was released in 2007 and before the Apple and Google app stores opened in 2008. With the dramatic increase in the use of smartphones and apps since that time, it is likely that the incidence of GPS stalking has increased. As an example of a Canadian case, in 2012 a Sault Ste. Marie police officer pled guilty to unlawfully using an electronic device to intercept the function of a computer system. The officer admitted to installing a stalking app on his wife’s cellphone, claiming that he hadn't known that it was illegal. Last year, the National Network to End Domestic Violence, in testimony before the US Senate Judiciary Committee, described how stalking apps are easily available on the internet, and gave several examples of their use.

---


193 Complaint for Damages, ibid at 4.


198 Linda Richardson, "City police officer pleads guilty to using spyware to track wife" (9 May 2012), Sault Star, online: <http://www.saultstar.com/2012/05/08/city-police-officer-pleads-guilty-to-using-spyware-to-track-wife>.

199 Cindy Southworth, "Testimony of the National Network to End Domestic Violence" (4 June 2014) at 4, online: <http://www.judiciary.senate.gov/imo/media/doc/06-04-14SouthworthTestimony.pdf>.
The related risk: data vulnerability

A related concern is the security, or lack thereof, of the location data collected by businesses, including the possibility of data breaches and cyber-attacks in relation to vast amounts of personal information shared with third parties:

Many companies are wary of giving third parties access to their data in case they are laxer about security or share it with competitors. In June Reuters, a news agency, had its website attacked by the Syrian Electronic Army through a third-party advertising network called Taboola which sat on its site. Others worry about a data breach from perhaps a rogue programmer who could de-anonymise the vast amount of information firms have collected.\(^{200}\)

An example is provided by the recent phenomenon of dating apps which use location data to match users. Cybersecurity firm Synack demonstrated a security vulnerability that allowed them to pinpoint the location of users of the gay dating app, Grindr, and indicated that other dating apps could be exploited in the same way.\(^ {201}\) It was reported that Egyptian police had used the Grindr vulnerability to track down and arrest gays in the country.\(^ {202}\) Grindr subsequently disabled location-tracking by the app in countries that have anti-gay laws.\(^ {203}\)

Stakeholder views

The Information and Privacy Commissioner of British Columbia (IPC-BC), in response to the report author’s consultation questions, acknowledged there are concerns:

Consumers should ensure they are informed about why information about their location is being collected and that they are comfortable with the purpose given. Consumers should also be concerned that this information may ultimately be shared or sold to other organizations and used for purposes that they are not aware. There is also the risk that location-based information can reveal an individual’s daily events or patterns of movement. Individuals should also be concerned about how long this information will be retained.

The Consumer Federation of America, in the stakeholder consultation, expressed the view that location information is “really one of the most sensitive things about you – where you go, who you associate with, what your activities are. It’s hard to think of anything that is more sensitive other than the contents of your [telephone] call.”

\(^ {202}\) Conor Sheils, “Egyptian Cops Using Grindr To Hunt Gays” (1 September 2014), Cairo Scene, online: <http://www.cairosscene.com/LifeStyle/Egyptian-Cops-Using-Grindr-To-Hunt-Gays>.
Professor Skillicorn, whose academic focus is “technical knowledge of data mining and its relationship to privacy” at the Surveillance Studies Centre at Queen’s University, believes that location information is very personal in nature.

[Location information] is very close to identification. If you know where someone spent the night, you’ve reduced the possibility of who they could be. It’s a very powerful piece of information relative to other information. Trajectory is just as important as location. With locations over time, you know even more. Because it’s a behaviour, that’s typically more important than even location and identification.

In Professor Skillicorn’s view, expressed in the stakeholder consultation, the problem is that with discrete bits of data, fingerprint-like profiles can nevertheless be created. He commented that he did not see much benefit to location information being tracked except for in emergency situations and for parents being able to monitor children (similar to views expressed by the Consumer Federation of America), saying that “most people don’t want other people knowing where they are.”

In Professor Skillicorn’s view, the privacy risk is not necessarily about individual bits of information, but the collection and correlation of discrete bits of information: “The real threat isn’t that individual pieces of information leak your information, it’s that discrete bits of location are being used to build profiles of you.”

In the view of Professor Skillicorn and Professor Steeves, there is an inequality of bargaining power over the tracking of location information. Professor Skillicorn noted that “it’s a take it or leave it proposition” for mobile services and apps - “your mobile device is actively reporting where it is, and apps all seem to want to track your location.” Professor Skillicorn as well as Professor Steeves noted that there is also a tendency toward digital monopolies, with fewer and fewer digital platforms (social media and search conglomerates) controlling more and more essential digital platforms, and gaining more and more control over massive amounts of personal information. As Professor Skillicorn noted, “opting out is not really an option.” In his view, “there is a power imbalance, and there’s no bargaining – people just buy or use the app.”

What’s more, in Professor Steeves’s view, there is a range of problems associated with people not being able to appreciate the harms (both direct and indirect, specific and more societal) that can flow from the vast amount of data being collected. “The problem is if you’re not in a position to understand the risk, you can opt-in to something you think is harmless, until you’re harmed by it.”

---

204 See also Jill Walker Rettberg, *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves* (Palgrave McMillan: 2014) at 81-82:

Avoiding being tracked and profiled by data brokers is not easy to do. In Dragnet Nation, Julia Angwin (2014) writes about how she tries to keep her data private, and she concludes that to not be tracked you have to have very sophisticated technical knowledge or have a lot of money. As Vertesi points out, many of the strategies you might legitimately use to stay private – such as using encryption or using cash instead of credit cards – are also likely to flag you as a potential criminal.
Rogers, the only TSP to participate in the stakeholder consultation, stated that “location-based information] is one of those things that people find creepy, so it has to be managed, so that’s the risk.” Rogers continued to suggest that “the thing that can seem creepy today can seem OK tomorrow ... when consumer preferences and tastes change.”

What do Canadians think about location-based information privacy?

This section reviews and reports on primary and secondary research on what Canadians think about location-based information privacy.

Canadians are concerned with protecting their privacy, generally. This is evidenced by the widespread concerns about the federal government’s previous attempt to update lawful interception legislation, and such initiatives as OpenMedia.ca’s “Protect our Privacy” grassroots campaign against the federal government’s Anti-terrorism Act.

In addition to this general concern with privacy, Canadians have been specifically becoming more concerned about their privacy in the context of telecommunications. Academics, civil society groups and citizens have all been increasingly voicing concerns over the data collection, use and sharing practices, for example, of telecommunications service providers, as extensively reported in the news media.

Prior consumer surveys

A 2011 OPC public opinion survey revealed that almost two thirds of Canadians (65%) agreed that protecting personal information will be one of the most important issues facing Canada in the next 10 years, and that roughly nine out of ten were concerned with businesses requesting

---


too much personal information, not keeping information secure, and selling it to other organizations.207

A 2012 consumer study commissioned by the Canadian Wireless Telecommunications Association, a trade group, found that only 22% of smart phone users were receptive to the idea of providing an app developer with either demographic or location-based information about themselves, in order to receive an app for free.208

In a 2012 guidance document entitled “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps,” the OPC and the British Columbia and Alberta Information and Privacy Commissioners commented on these studies, stating, “These findings demonstrate that Canadians are concerned about privacy in the mobile space.”209

The OPC’s Privacy Survey: 2014

Several findings in the OPC’s 2014 annual survey of Canadians’ views on privacy show that Canadians are deeply concerned about the risks mobile devices and location information pose:

- 75% of Canadians who use a mobile device expressed concern about what might happen to the personal information stored on their device if it is lost or stolen (49% are extremely concerned);
- 75% have decided not to install, or have uninstalled, an app because they were concerned about the personal information they would have to provide (up from 55% in 2012);
- 58% have turned off the location tracking feature on their mobile device (up from 38% in 2012); and
- 84% of Canadians are concerned about posting information about their location online, with 59% very concerned.210

The results regarding the voluntary disclosure of location information online, as illustrated by the following figures excerpted from the OPC’s report, are telling.

---


Concern over voluntary location information sharing is consistently the top concern, and concern is growing. It is reasonable to believe that if concern over voluntary location information sharing is high, then concern over involuntary or unknown location information tracking would also be high, if not higher by virtue of any lack of control or knowledge of the tracking. Indeed this is what PIAC’s own research revealed, as discussed in the next section.

These results are also in line with US data from the Pew Internet & American Life Project indicating that a significant majority of adult internet users has taken steps to avoid surveillance
online, and that “many mobile users of all ages say they have turned off location-tracking features at some point due to privacy concerns.”

**PIAC survey by Environics**

In 2014 PIAC commissioned Environics Research Group (Environics) to conduct a national telephone survey of Canadians’ attitudes towards location-based tracking. The telephone survey was conducted among a national random sample of 2,000 adults comprising 1,003 males and 998 females 18 years of age and older, living in Canada, between the 10th and 21st of September, 2014.

Environics posed seven questions to respondents. The questions were aimed at identifying respondents’ use of smartphones, and comfortableness with their location being tracked and with location-based marketing; their views relating to consent requirements; and their views on potential sanctions for violators of privacy rules. The margin of error for a sample of this size is +/- 2.19%, 19 times out of 20.

There is little doubt, as discussed earlier, that businesses see a tremendous opportunity in harnessing location information, and that some services based on location information may be attractive to consumers. However, many publicly available consumer surveys focus largely or solely on the business potential of location information, rather than Canadians’ broader comfort level with its collection, or the legal framework that can protect consumers from its misuse. Therefore, that was the emphasis of the Environics survey.

Generally, the results of the Environics survey indicate that:

- Canadians are uncomfortable with location-based information tracking (see e.g., Figure 6, showing 77% of respondents are very or somewhat uncomfortable);
- Canadians believe that location-based information is highly personal information, that requires explicit consent before it is collected and used (see e.g., Figure 8, Figure 10);
- Canadians’ concerns with location-based technologies fall into general privacy concerns but also the potential for specific harms resulting from the use or misuse of location information (see e.g., Figure 8, Figure 9); and
- Canadians believe that there should be consequences for violating privacy norms (see e.g., Figure 11).

A more detailed explanation of the results is provided as Appendix “A” to this report.

---

211 Pew Research Centre, “Location Based Services” (12 September 2013) online: <http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Location-based%20services%202013.pdf>.
212 See e.g. Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 99: “There is no doubt that many location-based services offer real benefits to users.”
Overall, Canadians clearly believe their physical location is being, or can be, tracked while they use their smartphones. A large number of Canadians (30%) do not know whether or not they are subject to location tracking when using their smartphones. This is consistent with the European Network and Information Security Agency’s view that “many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this.”\textsuperscript{213}

Canadians appear to be uncomfortable with receiving advertisements or coupons from retailers based on their location. Only 9% of total respondents said they were ‘Very Comfortable’ with the idea, and overall, nearly 2/3 of all Canadians (65%) are uncomfortable with receiving these kinds of offers.

While older age groups are significantly more uncomfortable with the idea of location tracking than the 18-29 group, and younger Canadians may be more amenable to smartphone-based location tracking than their older peers, they too are not particularly comfortable with the idea.

Only 13% of respondents expressed having no concern at all with location tracking. Of those who have concerns with location tracking, the greatest concern (32%) was about the invasion of privacy resulting from their location being tracked. Overall, respondents are concerned with \textit{general} privacy invasions more than they are concerned with specific harms resulting from privacy invasions.

In response to a question about the importance of consent before location tracking, the survey results indicate that Canadians, who generally are concerned about privacy, want to be in control of whether their location is being tracked, \textit{before} any tracking begins. Also the responses to the question, phrased as “…that you are \textit{always} asked…”, implies that Canadians would only be comfortable with a high level of consent, likely informed, explicit, opt-in consent. Combining the top 2 (“very important,” “somewhat important”) and bottom 2 response categories (“not at all important,” “don't know”), 91\% versus 8\% (at a 2.8\% margin of error) provides very little leeway for concluding otherwise. This result is strengthened taking into account the responses to the questions about Canadians’ overall comfort with location tracking and receiving coupons based on location tracking. Even those who may be comfortable with such tracking, it may be concluded, still wish to be in control of the collection and use of their location information.

Chapter 4 – Location-based technologies and the law

This chapter reviews and assesses the legal approach to privacy and location-based technologies in Canada, and explores approaches in other jurisdictions.

Canadian law

Statutes

This section surveys the Canadian legal landscape to determine what rules govern location-based technologies, the collection and use of location information, and evaluates whether the law as it currently stands can address consumers’ concerns with these practices.

PIPEDA

In Canada, PIPEDA governs the protection of personal information that is being collected, used or disclosed in the private sector for commercial purposes. According to the OPC, “PIPEDA sets out the ground rules for how private-sector organizations collect, use or disclose personal information in the course of commercial activities across Canada.” PIPEDA is based on 10 principles, including identifying purposes (principle 2), consent (principle 3), limiting collection (principle 4), limiting use, disclosure and retention and disclosure of personal information (principle 5), and safeguards (principle 7).

In the words of Industry Canada, “Privacy is a deeply-rooted, strongly-held public value. PIPEDA was enacted to alleviate consumer concerns about privacy and to allow Canada's business community to compete in the global digital economy. Organizations able to demonstrate their respect for, and protection of, personal information will gain a cutting edge on the competition. Complying with PIPEDA will build trust in the digital marketplace and create opportunities for Canadian businesses.”

In general, PIPEDA applies to organizations engaged in commercial activity, whether the activity crosses provincial borders or stays entirely within provincial borders. PIPEDA also applies to federally-regulated organizations engaging in commercial activity, and federal works and undertakings, such as banks or telecommunications service providers.

214 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 4(1).
215 Office of the Privacy Commissioner of Canada, “Privacy Legislation in Canada” (May 2014) online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>.
217 Office of the Privacy Commissioner of Canada, “Privacy Legislation in Canada” (May 2014), online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>. 
Location-based technology companies such as mobile service providers, mobile device manufacturers and sellers, and app developers are generally all engaged in commercial activities and as such are subject to PIPEDA. Location-based technologies exclusively used and offered in one province will likely fall under provincial legislation, if one exists. Even if the app itself does not actually generate revenue (i.e., free to download, no advertising), the collection of personal information to improve the commercial success of the app can still be considered commercial activity which subjects the app to PIPEDA.\textsuperscript{218}

PIPEDA does not apply, however, to commercial activities that take place wholly within a province, if the province has enacted legislation that is declared “substantially similar” to PIPEDA. Currently, only Alberta, British Columbia and Quebec have adopted legislation that has been declared substantially similar.\textsuperscript{219}

The OPC oversees PIPEDA in an ombudsperson-like role, and Industry Canada is responsible for the legislation to Parliament. The OPC’s enforcement powers, as the Office itself has admitted,\textsuperscript{220} are limited. A number of authors have recommended that the OPC be granted

\textsuperscript{218} Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps” (October 2012), online: <https://www.priv.gc.ca/information/pub/gd_app_201210_e.asp>. See also Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99 at 116: An app that is provided free of charge is in more of a grey area, although if the app collects personal information for the purposes of selling this data or using it in other commercial undertakings, this will no doubt be considered a collection in the course of commercial activity.

See also Office of the Privacy Commissioner of Canada, Interpretation Bulletin, “Commercial Activity”, online: <https://www.priv.gc.ca/leg_c/interpretations_03_ca_e.asp>.

\textsuperscript{219} Alberta’s Personal Information Protection Act, SA 2003, c P-6.5 was declared substantially the same by SOR/2004-219, British Columbia’s Personal Information Protection Act, SBC 2003, c 63 was declared substantially the same by SOR/2004-220, and Quebec’s An Act respecting the protection of personal information in the private sector, RSQ, c P-39.1 was declared substantially the same by SOR/2003 -374. Some provinces have enacted sector-specific legislation that has been deemed substantially similar to PIPEDA, such as Ontario, New Brunswick and Newfoundland and Labrador’s health-sector legislation; see Office of the Privacy Commissioner of Canada, “Privacy Legislation in Canada” (May 2014), online: <https://www.priv.gc.ca/leg_c/interpretations_03_ca_e.asp>.

\textsuperscript{220} The Office of the Privacy Commissioner of Canada, “The Case for Reforming the Personal Information Protection and Electronic Documents Act” (May 2013), online: <https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp>:

The days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise. It is time to put in place financial incentives to ensure that organizations accept greater responsibility for putting appropriate protections in place from the start, and sanctions in the event that they do not. Without such measures, the Privacy Commissioner will have limited ability to ensure that organizations are appropriately protecting personal information in the age of Big Data.
order-making power and the power to impose fines for non-compliance. Currently, the OPC is limited to making findings, and then applying to the Federal Court for an order.

In order for PIPEDA to apply to the collection, use or disclosure of personal information, the actions must occur in the context of commercial activity. Commercial activity is defined by PIPEDA as “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.” In the provincial privacy legislation, the definition is more nuanced, but generally captures the same or more types of activities.

In 2012, the House of Commons Standing Committee on Access to Information, Privacy and Ethics undertook a study on the efforts and the measures taken by social media companies to protect the personal information of Canadians, and reported the Committee’s findings and recommendations back to the House of Commons. The Committee, having heard from a range of witnesses and conducted meetings with a range of individuals and organizations about the issues, made six recommendations to increase privacy protections for Canadians. The focus of the recommendations was increasing transparency and control of personal information for social media users, and included concerns over location information, such as a user’s location attached to a social media post. The study also suggested the Privacy Commissioner should play a greater role in monitoring and guiding companies’ compliance with privacy law.

**Appropriate purpose**

Section 5(3) of PIPEDA limits, in theory, the collection of “personal information” by organizations “only for purposes that a reasonable person would consider are appropriate in the circumstances.”

What is an appropriate purpose has been given a broad interpretation, although the OPC has not produced an interpretation bulletin or legal guidance document on the subject.

A recent expression of the breadth of the “appropriate purpose” requirement is found in the OPC’s recent findings regarding Bell’s “Relevant Ads” program.

---

221 See e.g., France Houlse & Lorne Sossin, “Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act: An Effectiveness Study” (August 2010), online: <https://www.priv.gc.ca/information/research-recherche/2010/pipeda_h_s_e.asp>.

222 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s. 16.

223 Personal Information Protection and Electronic Documents Act, ibid s 2(1).

224 See Question 4, Office of the Privacy Commissioner of Canada, “Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia’s Personal Information Protection Acts” (5 November 2004), online: <http://www.priv.gc.ca/resource/fs-fi/02_05_d_26_e.asp>.

225 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, Privacy and social media in the age of big data (April 2013), online: <http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf>.
In our analysis of this issue, we have considered Bell's objectives in implementing the RAP [Bell's Relevant Ads Program], the likely effectiveness of the RAP in achieving those objectives, and the nature of the information used. We must also remain cognizant that the purpose of PIPEDA is to "establish...rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances".

With that in mind, we accept that Bell's objectives of maximizing advertising revenue while improving customers' online experience is a legitimate business objective. We also accept that the RAP may very well be effective in achieving those objectives. Studies like The Value of Behavioural Advertising, sponsored by the National Advertising Initiative, have found that behaviourally targeted ads are significantly more effective than random or contextual ads, and thus generate greater revenue for ad networks. The addition of account/demographic information to interest categories in Bell's Customer Profiles should serve to improve the precision and effectiveness of its targeting. We also appreciate that some users may prefer to see ads that are consistent with their interests and/or demographic characteristics.

Notably, the OPC conditioned this approval of Bell's business rationale on any subsequent CRTC assessment of the matter under telecommunications law. For the purposes of this paper, however, the emphasis of the OPC on the business gains possible through behavioural advertising, in the absence of any substantive discussion of the privacy rights of individuals, save for a mention that “some users” might prefer to receive targeted ads, begs the question about whether an appropriate balance has indeed been struck. At the same time, the privacy commissioners have also made this strong recommendation regarding apps: “Avoid collecting information about a user's movements and activities through the use of location and movement sensors unless it relates directly to the app and you have the user's informed consent.”

There appears to be a contradiction between the wide scope of information Bell had been authorized to collect (subject to the OPC's finding that opt-in consent was required), and the general recommendation against over-collection. The contours which define what is appropriate and what is inappropriate are unclear.

The need for consent

The foundational principle underlying PIPEDA is the requirement that informed consent be obtained for the collection, use and disclosure of personal information. Furthermore, collection of personal information must be related to a specific purpose: “The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected” (Principle 2). Consent must be obtained for any new purpose (Clause 4.2.4). In obtaining consent, the “reasonable expectations of the individual are also relevant” (Clause 4.3.5).


Obtaining consent has been observed to be a challenge in the mobile computing environment. As The Economist noted, “Consent to being tracked is more complicated on mobile phones, where firms’ privacy policy (assuming they have one) comes in very small print, and many consumers are not tech-savvy enough to know when their location is being monitored, even if they have agreed to it.”

The OPC, IPC-BC and IPC-AB for example have described the challenge as follows:

There’s been no shortage of discussion on the need to improve privacy rules and settings on the small screen of a mobile device. The challenge is to show users, in a creative and meaningful way, what is actually happening with their personal information. After all, no one wants to read a 20 page privacy policy on a small screen.

The privacy commissioners therefore provided some guidance on how businesses can obtain meaningful consent, despite the “small screen challenge,” through such techniques as “layering” information, providing a “privacy dashboard,” and using interactive graphics, colour and sound alerts to alert users to a “privacy-related decision that needs to be made in a timely way.” The privacy commissioners gave the example of how businesses “could also make use of graphics in the app at the moment when sensitive information is about to be transmitted and user consent is required.” For example, if your app is about to access the user’s location data, you could activate a symbol to raise user awareness of what is happening and the reason for it, as well as the user’s choices.

The privacy commissioners also emphasized that the timing of consent is important, recommending that businesses “tell users in advance what will happen with their information with the eventual use or deployment of the app and also in real time, while it’s actually happening” as one way to keep users informed on an ongoing basis. Again, the privacy commissioners used the example of location information: “For example, if your app is about to

---


The EU describes the problem succinctly as follows: “the consent for certain applications to use their location data is invalid, because the information about the key elements of the processing is incomprehensible, outdated or otherwise inadequate.” (EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 13/2011 on Geolocation services on smart mobile devices (adopted on 16 May 2011), online: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>, at 19)


231 Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, ibid.

232 Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, ibid.

233 Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, ibid.
actively access the user’s location data, you could activate a symbol to raise user awareness of what is happening."\textsuperscript{234}

In the view of the IPC-BC, expressed in the stakeholder consultation, consent for the collection if location information “would likely be required by PIPA.” Further, while PIPA does provide for implied consent in some circumstances, generally, where consent is required, it must be opt-in rather than opt-out.

In the view of the OPC, expressed in the stakeholder consultation, “PIPEDA is principles-based legislation which requires a case-by-case analysis.” Then, “context is one element of the analysis, in combination with other factors,” and “depending on these factors, there could be a possibility for location to be sensitive.”

\textit{“Personal information” defined}

Location information is not explicitly addressed in PIPEDA, nor in any provincial privacy legislation. Privacy commissioners’ decisions and court interpretations determine, based on the context, whether location information falls under the definition of “personal information.”

According to PIPEDA, “personal information” is defined as “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.”\textsuperscript{236} Alberta’s \textit{Personal Information and Protection Act (AB-PIPA)} defines “personal information” as “information about an identifiable individual,”\textsuperscript{236} while British Columbia’s \textit{Personal Information and Protection Act (BC-PIPA)} defines it as “information about an identifiable individual and includes employee personal information but does not include contact information or work production information.”\textsuperscript{237} Lastly, Quebec’s privacy law defines personal information as “any information which relates to a natural person and allows that person to be identified.”\textsuperscript{238} These statutory definitions have been given broad and expansive interpretations by the courts,\textsuperscript{239} with the key element being that the information must be reasonably capable of identifying a particular individual either alone or when combined with information from other available sources.\textsuperscript{240}

\begin{itemize}
  \item \textsuperscript{234} Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, \textit{ibid}.
  \item \textsuperscript{235} \textit{Personal Information Protection and Electronic Documents Act}, SC 2000, c 5, s 2(1).
  \item \textsuperscript{236} \textit{Personal Information Protection Act}, SA 2003, c P-6.5, s 1(1)(k).
  \item \textsuperscript{237} \textit{Personal Information Protection Act}, SBC 2003, c 63, s 1.
  \item \textsuperscript{238} \textit{An Act respecting the protection of personal information in the private sector}, RSQ, c P-39.1, s 2.
  \item \textsuperscript{239} See e.g. \textit{Dagg v Canada (Minister of Finance)}, [1997] 2 SCR 403, La Forest J, dissenting, at para 68; \textit{Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)}, 2006 FCA 157.
  \item \textsuperscript{240} See e.g. \textit{Ontario (Attorney General) v Pascoe} (2001), 154 OAC 97 (Ont Div Ct), aff’d \textit{Ontario (Attorney General) v Pascoe}, [2002] OJ no 4300, 166 OAC 88 (Ont CA); \textit{Gordon v Canada (Health)}, 2008 FC 258.
\end{itemize}
The higher standard for “sensitive” personal information

“Sensitive” personal information is a particular category of personal information that requires a higher level of protection under PIPEDA, but is not defined by PIPEDA or any equivalent provincial law. (The PIPA-BC also has a concept of “sensitivity” related to assessing the reasonableness of collection, use and disclosure is appropriate, and in relation to required security measures.241) PIPEDA, states that some information such as medical records and income records will almost always be considered to be sensitive, and suggests that any information can in fact be sensitive depending on its context.242 Interestingly PIPEDA also states that “the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.”243 Context is a determining factor of the sensitivity of the information, which can be observed by the following decisions.

It remains to be seen whether the law requires that location-based technologies obtain express consent if they collect location-based personal information from individuals, although some of the previous findings and guidance from the privacy commissioners suggests location may be considered sensitive on an absolute basis, despite the contextual approach required by the privacy statutes.

Privacy Commissioner findings and guidance relating to location

Canadian privacy commissioners have had only limited occasion on which to interpret the status of location information, including some cases which only relate to the employment context rather than the business to consumer context.


Note however, as the IPC-BC stated in the stakeholder consultation:

For the most part, PIPA treats all personal information the same. If something is personal information, then the rules regarding collection, use and disclosure apply regardless of the sensitivity. The one exception is that the reasonable security arrangements that must be in place do vary based on the sensitivity of the personal information involved. This is something that again would need to be looked at on a case-by-case basis, but there are certainly instances where location-based information could be quite sensitive. For example, this could be the case in instances such as where it relates to individuals that are seeking to escape abuse or reside at transition houses.

242 PIPEDA, supra note 4, Schedule I, s 4.3.4.
243 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, Schedule I, s 4.3.4 (emphasis added).
Location information as “personal information”

The question of whether location information is or capable of being “personal information” has been considered, at least theoretically, in only a number of privacy commissioner cases.

In Re Schindler\(^{244}\) the IPC-BC considered whether information collected from a vehicle fleet management system was being collected in compliance with BC-PIPA. The information collected included GPS-derived vehicle location information and information about the operation of the vehicle, including distance travelled, speed, harsh braking, sharp acceleration, and time in operation. The IPC-BC concluded that GPS location information is in fact “personal information.”\(^{245}\) As the Commissioner explained, the GPS data disclosing the location of the vehicle was about the vehicle, but the GPS location data also disclosed the whereabouts of the employee \textit{at any given time}, therefore making it reasonably capable of identifying an individual.\(^{246}\) As explained earlier, this signifies that the time dimension of location-based information is relevant, if not central to the privacy analysis.

While the argument could be made that mobile device location tracking reveals only the information of the mobile device and not the individual, the location data obtained from the device is reasonably capable of identifying the owner of the device. Even if an individual is not specifically named, as long as it is possible to make the identifying link, it becomes “personal information.”\(^{247}\) Unlike a vehicle, the sharing of a mobile device is more rare due to the intimate personal link to a specific individual thereby making the identification of an individual more palpable.\(^{248}\) Indeed, as described in Chapter 2, a key capability of location-based technology businesses is a detailed profile of the \textit{individuals} captured within the system; data which is then aggregated.

In a subsequent case, Re Kone,\(^{249}\) the IPC-BC’s conclusions on location information were further clarified, at least in the context of an employment relationship. The presiding adjudicator concluded that the location information gathered from the employees’ phones was “personal information.” The phones, equipped with GPS, were assigned to specific employees and were used in a way to specifically identify their movements, regardless of whether the phone was used for attendance purposes or for managing employee relationships, and even if the employees were not identified at all times to all users of the system.\(^{250}\) Although location-based technologies may not use location data obtained by a device’s GPS and may not be specifically targeting known individuals, it may nonetheless be possible to identify an individual by reviewing

\(^{244}\) Schindler Elevator Corp. (Re), 2012 BCIPC 25 (CanLII), <http://canlii.ca/t/fvfdl> [Re Schindler].

\(^{245}\) Re Schindler, ibid at para 112.

\(^{246}\) Re Schindler, ibid at paras 108-109.

\(^{247}\) University of Alberta v Alberta (Information & Privacy Commissioner), 2009 ABQB 112 at para 67.


\(^{249}\) Kone Inc (Re), 2013 BCIPC 23 (CanLII), <http://canlii.ca/t/g0hdk> [Re Kone].

\(^{250}\) Re Kone, ibid at para 17.
their patterns of movement and drawing inferences about the location of an individual’s home and workplace, thus constituting “personal information.”

These decisions provide support for the view that mobile location information, random or specific, is considered “personal information” as described in BC-PIPA, which is substantially similar to PIPEDA. Although these decisions were based on employment relationships, which given the intent of the programs in question may have made it much more easy for the employers to know the identities of who was being tracked, these decisions may illustrate how privacy regulators may consider location information more broadly.

Indeed, in a 2012 guidance document entitled “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps,” the OPC and the IPC-BC and IPC-AB recognized that location information could be “personal information.”

In the view of the IPC-BC, expressed in the stakeholder consultation, “So long as the location-based information is ‘information about an identifiable individual,’ it will be personal information under PIPA. In most instances, this will likely be the case (unless the information is truly anonymized), although it would have to be looked at on a case-by-case basis.”

In another OPC investigation concerning Google’s Android mobile device operating system, which involved extensive collection of a “broad range of information” including “search terms, recordings of a user’s voice, device location, calendar entries, and email”, the OPC found that “much of this information can be linked to a specific individual, either alone or in combination with other information available to Google.” Included in the findings was the recognition that Google was automatically collecting location information on certain devices (where the operating system was pre-installed), and using current and historical locations for customization and personalization of search results and personal reminders and information about such things as estimated travel times to given locations, as part of at least one app. Despite the extensive collection and use of location information recognized in the findings, the OPC did not specifically address location, or specific combinations of location with other information, but rather seemed to suggest the possibility of location being used to personally identify a person may be sufficient for deeming all location information “personal information”. In future finding a more specific discussion of location information collection and use could assist in clarifying the exact legal nature of location information.


253 PIPEDA Report of Findings #2014-008 (Agreement to an app’s “permissions” does not, by itself, equal consent to collect, use and disclose personal information - Google encouraged to provide users with greater clarity to avoid misperception), online: <https://www.priv.gc.ca/cf-dc/2014/2014_008_0529_e.asp>. ibid., at paras. 35, 64, and 78.
Location information as “sensitive” personal information

In PIPEDA Case summary 2009-011, for example, the OPC found that the information collected using mobile data terminals with GPS devices in vehicles the complainant drove for a municipal transportation service available to mobility-reduced citizens, was “personal information,” but not sensitive. This conclusion was reached because the primary purpose of the system was to legitimately improve dispatch efficiency, route rescheduling and vehicle arrival times.\(^{255}\)

In *Re Kone* (2013), the increased accuracy of the GPS location information from the mobile phones made the location information more sensitive. Nonetheless, the sensitive nature of the information was diminished because the type of location information was relating to employees during work hours in the context of work activities. Even so, the adjudicator left room for further interpretation of sensitive information by suggesting that if the location information of the employees was collected during lunch breaks, while attending personal appointments or while not working it would remain sensitive.\(^{256}\) This supports the principle that location information obtained from mobile devices for non-work related purposes may likely be considered sensitive.

In other OPC decisions the collection or sharing of location information has been described in the hypothetical sense, without actually concluding that the possible use of location information rendered it “personal information.” \(^{257}\)


\(^{256}\) *Kone Inc (Re)*, 2013 BCIPC 23 (CanLII) at paras 49-52, <http://canlii.ca/t/g0hdk> [Re Kone].

\(^{257}\) See PIPEDA Report of Findings #2011-001 ([Google Inc. WiFi Data Collection]), online: <https://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.asp>. This investigation into Google by the OPC was initiated as a result of revelations that Google had unlawfully collected personal information from unsecured wireless networks in several countries, including Canada. This unlawful collection occurred, according to Google, unintentionally during data-gathering by Google “Street View” cars for its location-based services. It was intended that the Street View cars, while driving on and mapping streets, would collect publicly broadcast SSID information and MAC addresses from WiFi networks and routers for the purposes of Google’s geolocational services. However, while collecting this location-based information, Google’s software inadvertently also collected “payload” data, which is the content of the communications that were occurring on the WiFi networks. The OPC found that Google was in contravention of PIPEDA as a result of failing to limit collection of personal information to that which was necessary for an identified purpose, failing to identify and disclose the purpose of collecting the personal information, and failing to obtain the consent of the individuals whose personal information was collected. The OPC made several recommendations to reduce the risk of future privacy violations.

See also PIPEDA Report of Findings #2013-017 ([Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising]), online: <https://www.priv.gc.ca/cf-dc/2013/2013_017_1120_e.asp>: The complainant alleged that Apple used her personal information for tracking purposes in the form of a unique device identifier (UDID) and an “Ad ID” without her knowledge and consent. The OPC found that UDIDs and Ad IDs were used by Apple, and disclosed to third party app developers for the purpose of delivering targeted advertising to Apple device users. In that context, the OPC viewed UDID, which could include location information, to be sensitive personal information as it could be used to create a detailed user profile. Accordingly the OPC recommended, among other things, that the device user be given a “just-in-time” notice and opportunity to consent to the disclosure of the UDID or Ad ID to third parties.
In the joint guidance from the OPC, IPC-BC and IPC-AB on the subject of privacy practices for mobile apps, discussed above, also seems to suggest that those privacy commissioners consider location to be inherently sensitive, although they do not appear to have conclusively stated as much but rather recognized the possibility that location may be sensitive personal information.\(^{258}\)

Indeed, in the stakeholder consultation the OPC that “there is the possibility for location information to be considered sensitive” – thus location is possibly “sensitive”, but not necessarily.

Most recently, in its findings about Bell’s “Relevant Ads” program, the OPC appeared to recognize the possibility that the collection and use of location information, as part of a broad behavioural advertising program, could render the information collected more sensitive than the individual pieces of information:

\[\text{[T]he sheer breadth of information being used or contemplated for the RAP (including internet, telephone and television network usage information, as well as account/demographic information) renders such information more sensitive when compiled. Bell should obtain express consent for the use of sensitive information.}}\(^{259}\)

The OPC also found that Bell had insufficiently explained how it would be collecting and using location information, and recommended (despite Bell not appearing not to have any specific plans to use location information for behavioural advertising in the future) that Bell obtain meaningful informed consent for any future uses of other information, including that related to mobile location.\(^{260}\) The basis for that recommendation, however, is unclear, whether it is based on a contextual analysis of the combined potential value of the information collected (website

_____________________

See PIPEDA Report of Findings #2013-001 (Investigation into the personal information handling practices of WhatsApp Inc.), online: <https://www.priv.gc.ca/information/pub/gd_app_201310_e.asp>. In the context of the WhatsApp social media app, the automatic sharing of status messages with anyone who had the user’s phone number was a concern of the OPC. These status updates could conceivably include information about a user’s location, if the user chose to share such details in the text of the update. See para. 61:

\[\text{In keeping with the interpretation of personal information above, we believe that information contained in a user's status submission may constitute personal information. There are innumerable instances where a user may elect to share information about him or her self – whether location, opinion, the status of a relationship, or some other self-expression – and where such information, alone or in combination with other data, would render the individual identifiable.}\]


\(^{260}\) Office of the Privacy Commissioner of Canada, “Results of Commissioner Initiated Investigation into Bell’s Relevant Ads Program” (7 April 2015), PIPEDA Report of Findings #2015-001, online: <https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_e.asp>, at paras. 18(b) and 115.
Specific laws governing telecom service providers

Telecommunications service providers (TSPs) are subject to a number of specific laws and requirements above and beyond PIPEDA – namely, the *Telecommunications Act*. 261

Section 7 of the *Telecommunications Act* enumerates nine policy objectives that codify and guide the development of telecommunications policy in Canada. Among them is an explicit reference to the protection of privacy:

> 7. It is hereby affirmed that telecommunications performs an essential role in the maintenance of Canada’s identity and sovereignty and that the Canadian telecommunications policy has as its objectives


As described in Chapter 2, some location-based technologies use customized Wi-Fi or Bluetooth systems in order to communicate with mobile devices or identify the radio frequencies emitted by mobile devices. Under the *Radiocommunication Act*, it is prohibited to install, operate or possess a radio device intended for use of radiocommunications unless the device (1) is authorized by a licence; (2) is a radio apparatus for the reception of broadcasting; or (3) is exempted under the Act or its regulations: *Radiocommunication Act*, s 4(1).

As described in Chapter 2, some location-based technologies use customized Wi-Fi or Bluetooth systems in order to communicate with mobile devices or identify the radio frequencies emitted by mobile devices. Under the *Radiocommunication Act*, it is prohibited to install, operate or possess a radio device intended for use of radiocommunications unless the device (1) is authorized by a licence; (2) is a radio apparatus for the reception of broadcasting; or (3) is exempted under the Act or its regulations. Sensors and beacons using Wi-Fi and Bluetooth technology appear to fall within the third exception for exempted apparatus. These radio devices are exempt from having to obtain a radio licence since these technologies fall within Industry Canada’s regulation for low-power licence-exempt radiocommunication devices. As long as the device meets specific technical parameters approved by Industry Canada, and operates within those parameters in practice, these devices are not regulated any further.


However, section 5(1.1) of the *Radiocommunication Act* provides a link to Canada’s policy objectives as set out in section 7 of the *Telecommunications Act*. While Industry Canada does not regulate the applications of exempt devices, in deciding what types of devices and their technical parameters should be exempt from licensing, Industry Canada could have regard to the protection of privacy policy objective. Should a particular class of devices become used primarily for purposes that violate the privacy of Canadians, Industry Canada could deny or remove an exemption for that class of devices. This would effectively prevent certain privacy-violating applications from legally operating in Canada. Such a decision would be a drastic move; however, Industry Canada retains the authority to do so. It remains to be seen if the collection of personal data by third parties via Wi-Fi and Bluetooth and other exempt radio equipment may is offside any of these requirements.
As a result, the CRTC has repeatedly held TSPs to a high standard of privacy in their dealings with consumers' information. Decisions stretching back to 1986 severely limit the circumstances under which TSPs can disclose “confidential customer information”\(^{262}\) to other entities, including the police, and until recently, affiliate companies of the TSP.\(^{263}\)

The OPC has also recognized the role the CRTC has to play in regulating TSPs with respect to consumer privacy. In a submission to the CRTC’s “Review of the Internet traffic management practices of Internet service providers” proceeding, the OPC noted:

> The CRTC has a statutory obligation and recognized expertise to protect privacy. …

PIPEDA represents a basic standard for how organizations should manage personal information. The CRTC, through its regulatory powers may exceed PIPEDA’s standard if, in their expert opinion, the proposed requirement is consistent with the public interest and Canadian telecommunications policy, as set out under the *Telecommunications Act*.\(^{264}\)

As of the date of this report, a complaint by PIAC and the Consumers’ Association of Canada regarding the lawfulness of Bell’s behavioural marketing program, which identified location as a possible data point, is still before the CRTC.\(^{265}\)

**Statutory tort of invasion of privacy**

Four Canadian provinces have passed laws which specifically create a civil tort for the invasion of privacy: British Columbia,\(^{266}\) Manitoba,\(^{267}\) Newfoundland\(^{268}\) and Saskatchewan.\(^{269}\)

---

262 Defined very broadly as “… all information kept by the Company regarding the customer, other than the customer’s name, address and listed telephone number …”


264 Office of the Privacy Commissioner of Canada, “Review of the Internet traffic management practices of Internet service providers; Final reply of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC)” (July 2009), online: <https://www.priv.gc.ca/information/research-recherche/sub/sub_crtc_090728_e.asp>.


266 Privacy Act, RSBC 1996, c 373.

267 Privacy Act, RSM 1987, c P125.

268 Privacy Act, RSNL 1990, c P-22.
The declaration and structure of each statutory tort is substantially the same:

It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual.

None of the statutes describe specifically what actions violate an individual's privacy. Some statutes provide exceptions, defences or criteria to be used in assessing a violation; however, they are vague definitions subject to interpretation. Therefore, it is up to the courts to determine on a case-by-case basis whether a specific action, in the circumstances, violates an individual's privacy. Whether the surreptitious gathering and use of location information would be considered a tortious violation of privacy under these statutes would depend heavily on the context under which it is collected.

In addition, Quebec's Civil Code, and the Quebec Charter of Human Rights and Freedom create privacy rights, under which a consumer can sue if their rights are breached. The Civil Code enumerates specific actions that are invasions of privacy, for example:

36. The following acts, in particular, may be considered as invasions of the privacy of a person:

... (4) keeping his private life under observation by any means;

Given the extremely broad nature of the language “by any means,” it appears location-based technologies would certainly be subject to this provision. Whether location-based technologies constitute an invasion of privacy then would depend on the specific circumstances under which the location information is collected. It is not clear that there would be an invasion of privacy in general due to the use of “private life.” For example, would a Wi-Fi tracking system operating in a public mall be observing the “private life” of an individual, given that they are in a public space? PIAC is not aware of any cases that have addressed this or similar questions, however, with the increasing use of location-based technologies, it may only be a matter of time before these issues come before a court.

**Common Law**

In addition to the previously described divergence amongst the provinces in terms of recognition of a statutory invasion of privacy tort, the common law in Canadian provinces diverges on the existence of a common law civil claim for violations of privacy.

---

271 Nymity, ibid.
In 2012, the Ontario Court of Appeal recognized a new tort of invasion of privacy, known as “intrusion upon seclusion,” in *Jones v Tsige*. The Court of Appeal overturned the lower court’s decision, finding that the Court was “presented in this case with facts that cry out for a remedy,” and recognized a right to bring a civil action for damages for the invasion of personal privacy.

The Court explained that privacy is of such a fundamental value to Canadians, that it warrants protection in the face of ongoing technological change. The court noted the three distinct privacy interests that the Supreme Court of Canada has recognized in cases involving the *Charter*, namely “personal” privacy, “territorial” privacy and “informational” privacy, the last of which was the subject of Jones’s complaint.

The Court described “informational privacy” as follows:

> [T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Its protection is predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit.

Despite no tort existing for the invasion of privacy previously, the Court ruled that it was necessary to recognize a new tort:

> The explicit recognition of a right to privacy as underlying specific Charter rights and freedoms, and the principle that the common law should be developed in a manner consistent with Charter values, supports the recognition of a civil action for damages for intrusion upon the plaintiff’s seclusion.

The Court then defined the three key elements of the tort a plaintiff must prove:

---

272 *Jones v Tsige*, 2012 ONCA 32.
273 *Jones v Tsige*, *ibid* at para 69.
275 *Jones v Tsige*, 2012 ONCA 32 at para 41 [citations omitted]: Charter jurisprudence has recognized three distinct privacy interests: Dyment; *R. v. Tessling*. The first two interests, personal privacy and territorial privacy, are deeply rooted in the common law. Personal privacy, grounded in the right to bodily integrity, protects “the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal”. Territorial privacy protects the home and other spaces where the individual enjoys a reasonable expectation of privacy. The third category, informational privacy, is the interest at stake in this appeal.
276 *Jones v Tsige*, *ibid*.
277 *Jones v Tsige*, *ibid* at para 46.
The key features of this cause of action are, first, that the defendant's conduct must be intentional, within which I would include reckless; second, that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.278

The Court was careful to place limitations on the circumstances under which the tort could be used. For example, a plaintiff can only sue for “deliberate and significant invasions of personal privacy,” intruding into matters such as financial or health records, sexual practice and orientation, employment, diary or private correspondence.279 It remains to be seen whether the tort of intrusion upon seclusion could exist in the context of businesses using location information, however given the intimate details which behavioural marketing is capable of capturing, it may be possible, although for a claim to be launched the individual would have to know about the intrusion in the first place, which may be problematic especially with regards to third parties.

Subsequent to Jones v Tsige, the British Columbia Court of Appeal in Demcak v Vo280 considered the same issue of a violation of privacy, albeit in a very different context (landlord and tenant dispute). However the court ruled against recognizing a new tort, holding, “No common law tort of invasion or breach of privacy exists in British Columbia.” The Court pointed instead to British Columbia’s statutory tort.281

In other analyses of this case, lawyers have suggested that the basis of the argumentation at trial, and the court’s reasoning, perhaps may have resulted in a decision which perhaps may in the future be revisited on more substantial grounds:

It is worth noting that the plaintiff in Demcak v Vo was a self-represented litigant whose two previous statements of claim connected to this matter had been struck out by Masters. The plaintiff did not specifically argue invasion of privacy, the court’s decision was very short, and one can be fairly certain that legal doctrine was not robustly argued at the hearing.282

In Alberta, where there is no statutory tort for the invasion of privacy, a court ruled in 2011 that Alberta does not have a common law tort for the invasion of privacy.283 The court there adopted the reasoning of a previous trial-level decision, which itself relied on an older British Columbia Court of Appeal decision.284 Instead, the Alberta court stated the complainant had to first file a complaint with Alberta’s Information and Privacy Commissioner. Since all of these decisions

278 Jones v Tsige, ibid at para 71.
279 Jones v Tsige, ibid para 72.
280 Demcak v Vo, 2013 BCSC 899 (CanLII).
281 Demcak v Vo, ibid at paras 8-9.
283 Martin v General Teamsters, Local Union No. 362, 2011 ABQB 412 (CanLII).
284 Martin v General Teamsters, Local Union No. 362, ibid at paras 43-48.
were made before the Ontario Court of Appeal’s decision in *Jones v Tsige*, it remains to be seen how the next case brought before the Alberta courts will be decided.

The implications of these decisions are still being explored. However, a class action, based in part on the intrusion upon seclusion tort, has been filed in Ontario against Bell Canada in relation to its “Relevant Ads” program.\(^ {285} \)

### How do other jurisdictions’ laws treat location information?

This section considers how the United Stated, the European Union, and the United Kingdom have addressed location-based information privacy. The approaches taken elsewhere may be instructive to any future consideration of the issue in Canada.

#### United States of America

In the United States a slightly different story is unfolding. There appears to be a growing concern for location information privacy, expressed by a number of litigants before U.S. courts, and by most states having recognized a right of action for invasion of privacy right. Unfortunately, most of the jurisprudence to date relates to individuals’ privacy rights vis-à-vis the state, not vis-à-vis businesses, however that prompts the question of whether businesses should be held to lower standards than the state when it comes to location-based privacy, particularly in the instance where businesses that collect and use location information may themselves be the target of state-based information collection processes.

An early case in the recognition of location privacy was the Fourth Amendment case of the Supreme Court of the United States in *United States v Jones* (2012).\(^ {286} \) In this case, it was determined that the Federal Bureau of Investigation had performed illegal tracking when it installed a GPS device on the suspect’s car for 28 days without a warrant or the suspect’s consent. The concurring opinion held that “the short-term monitoring of a person’s movements on public streets accords with expectations of privacy” while the “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy” as was the case with 28 days of monitoring.\(^ {287} \)

Following the *Jones* decision, in July of 2013, New Jersey’s highest court, the Supreme Court of New Jersey, issued a landmark decision in *State v Earls*, where it held that individuals have a reasonable expectation of privacy with regards to their mobile phone location data based on the state’s constitution. The court unanimously concluded that "cell-phone location information, which users must provide to receive service, can reveal a great deal of personal information

---


\(^{286}\) *United States v Jones*, 132 S Ct 945 (2012).

\(^{287}\) *United States v Jones*, ibid.
about an individual ... [y]et people do not buy cell phones to serve as tracking devices or reasonably expect them to be used by the government in that way.\textsuperscript{288}

More recently, in 2014, the Massachusetts Supreme Judicial Court, Massachusetts’s highest court, held in \textit{Commonwealth v Augustine} that an individual has a constitutionally protected reasonable expectation of privacy in cellular phone location records, and that the Commonwealth of Massachusetts was required to obtain a search warrant prior to obtaining such information.\textsuperscript{289}

Concerns about location privacy have prompted US federal lawmakers to act. While there is currently no enacted legislation on location information, there recently have been three separate but similar proposed federal Bills tabled, each dealing specifically with the protection of personal location information. The Consumer Federation of America, in the stakeholder consultation, noted that unlike Canada or Europe, the US does not have comprehensive privacy legislation.

The first of the three is the Geolocation Privacy and Surveillance Act (the GPS Act)\textsuperscript{290}, which was introduced on March 21, 2013. The proposed act intends to apply to any person, including covered services (\textit{i.e.}, electronic communication service, remote computer service, or geolocation information service) and would criminalize the intentional interceptions or disclosures of geolocation information pertaining to another person unless the individual in question has given prior consent.\textsuperscript{291} There are many exceptions to this rule such as the interception by a parent or legal guardian, the interception by law enforcement officers or emergency responders, as well as the location information being public knowledge.\textsuperscript{292} In addition, the interceptions by covered services contain various loopholes such as the right to divulge information that was inadvertently obtained and which appears to pertain to the commission of a crime.\textsuperscript{293} The Bill also allows for a private right of action with minimum statutory damages for those concerned at $10,000,\textsuperscript{294} while prohibiting the acquisition of geolocation information for public safety purposes (“protective activities or law enforcement or intelligence purposes”) except pursuant to a warrant.\textsuperscript{295}

What is noteworthy about the Bill is its definition of geolocation information:

> The term "geolocation information" means, with respect to a person, any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device that, in whole or in part,
is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.²⁹⁶

In contrast, the similar proposed Online Communications and Geolocation Protection Act²⁹⁷ (the OCGP Act) includes the following definition of geolocation:

The term ‘geolocation information’ means, with respect to an individual, any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the present, prospective, or historical location of the individual.

Notably this definition includes a temporal aspect to the geolocation information - regarding the present, prospective or historical location of the individual.²⁹⁸ Also, notably, this definition appears to capture what is commonly referred to as “metadata” or “data about other data,” and indeed the Privacy Commissioner of Australia recently ruled that metadata held by Telstra, a large Australian TSP, including location-based information itself is “personal information” under Australia’s Privacy Act, from which an individual’s identity could reasonably be ascertained despite it being lengthy and complex to do so.²⁹⁹

While comparable to the GPS Act, the OGGP Act varies slightly in addition to definitions. The GPS Act targets all persons, while the OCGP Act targets solely governmental access and not commercial access of location information.³⁰⁰

The third Bill, the Location Privacy Protection Act of 2014 was proposed in March 2014, after the backlash from the tracking of consumers as they shopped by a location-based technology company.³⁰¹ The Bill, resembling the British and European regulations, would prohibit businesses from collecting, using and disclosing location information from an electronic communications device without affirmative express consent.³⁰² Companies collecting information from more than 1,000 individuals would have to maintain a publicly accessible internet website that includes the type of geolocation information that was collected from electronic communications devices; the purposes for the collection, use or disclosure; if information was disclosed, to whom it was disclosed; and how an individual may revoke his or

²⁹⁶ US, Bill S 237, ibid, s 2 (§ 2601(4)).
²⁹⁷ US, Bill HR 983, Online Communications and Geolocation Protection Act, 113th Cong, 2014 [OCGP Act]. The Bill died in a previous Congress and was reintroduced on 2 February 2015: US, Bill HR 656, Online Communications and Geolocation Protection Act, 114th Cong, 2015.
²⁹⁸ US, Bill HR 656, ibid, s 3 (§ 2601(3)).
³⁰⁰ Ben Grubb and Telstra Corporation Limited, ibid, s 3 (§ 2602(a)).
³⁰² US, Bill S 2171, Location Privacy Protection Act of 2014, 113th Cong, 2014, s 3 (§ 2713(a)(2)).
her consent. 303 Failure to comply with the provisions can leave an entity with a maximum penalty of $1,000,000 if the conduct was not found to be willful or intentional. 304

In the stakeholder consultation, the Consumer Federation of America suggested that the reason there have been a number of different location information bills tabled is because “legislators have realised getting a comprehensive privacy bill through Congress is a really heavy lift, so it might be easier to get through some more narrowly focussed legislation. Given the explosion in smartphone usage and apps, it seems like a logical development.” The Consumer Federation of America also noted that location arguably fits with the Telecommunications Act of 1996 definition, and the FCC’s interpretation, of “customer proprietary network information” (CPNI).

**European Union**

EU Directive 2002/58 treats the processing of “personal data”, but is only applicable to telecommunications service providers and not to third parties. 305 Article 9 of the Directive restricts the processing of “location data” only to cases where an individual can retain his or her anonymity or with consent from the individual when value added services are necessary. Providers must also include all relevant information with regards to the processing of location information as well as the freedom to withdraw consent. 306 The Directive places strict limits on the use of location information for only the purpose of the value-added service in question, and appears to require ongoing, affirmative consent by the user. The Directive also requires informed consent for the processing of their location data for the provision of value-added service by third parties.

The European definition of “location data” is non-exhaustive. The definition states that “location data may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the

303  US Bill, S 2171, ibid, s 3 (§ 2713(b)(4)).
304  US Bill, S 2171, ibid, s 3 (§ 2713(d)(4)(A-B)).
306  EU Directive 2002/58, ibid, art 9, s 1:

Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.
network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.”

The Directive was supplemented with an additional provision, which states that EU member states will have to store individual’s telecommunications data (which includes location data) for a minimum of 6 months and a maximum of 24 months. There is an exception to the consent requirement for emergency response and law enforcement “override” to the consent requirement.

In a subsequent opinion in 2011 by the EU’s Data Protection Working Party, the Working Party reiterated that location information from smart mobile devices are personal data” and that the combination of the unique MAC address and the calculated location of a Wi-Fi access points should also be treated as personal data. The Working Party also made extensive recommendations about the collection, use and retention of location information, including the following:

Because location data from smart mobile devices reveal intimate details about the private life of their owner, the main applicable legitimate ground is prior informed consent.

Consent cannot be obtained through general terms and conditions.

Consent must be specific, for the different purposes that data are being processed for, including for example profiling and or behavioural targeting purposes from the controller. If the purposes of the processing change in a material way, the controller must seek renewed specific consent.

By default, location services must be switched off. A possible opt-out mechanism does not constitute an adequate mechanism to obtain informed user consent.

Data subjects must be able to withdraw their consent in a very easy way, without any negative consequences for the use of their device.

The different controllers of geolocation information from mobile devices should enable their customers to obtain access to their location data in a human readable format and allow for rectification and erasure without collecting excessive personal data.

Data subjects also have a right to access, rectify and erase possible profiles based on these location data.

---

Like the U.S., the EU appears to have recognized the concerns over location privacy and taken steps to regulate it. Unlike the U.S., the EU appears to have had more success in that regard, as has the United Kingdom, as briefly described in the next section.

**United Kingdom**

The United Kingdom is also actively engaged in the regulation of location information with the introduction of UK Regulation 14, under the European Commission’s *The Privacy and Electronic Communications (EC Directive) Regulations 2003* which imposes certain restrictions on the processing of location data.\(^{311}\) Location information or “location data” as it is called in the British legislation, is defined as “any data processed in an electronic communications network which indicates the geographical position of the terminal equipment of a user.”\(^ {312}\)

The U.K. regulation allows the processing of location information by electronic communication providers only if the individual cannot be identified from such data or with the consent of the individual if there is a value added service.\(^ {313}\) Prior to the processing the provider must obtain consent by informing the user about the type of location information that will be processed, the purpose and duration of the processing, and whether the location information will be transmitted to a third party. Lastly, an individual has the right to withdraw his consent at any time using a simple means and free of charge.\(^ {314}\)

**Prior research**

A number of Canadian authors and institutions have previously considered the suitability of the legal and regulatory framework applicable to location-based technologies.

In a 2005 report to the OPC, Professor Colin Bennett and Lori Crowe foretold the growing challenge to Canadian law of location tracking.\(^ {315}\) In their report, Bennett and Crowe concluded that “it is commonly agreed that privacy advocates and regulators in all countries need to concentrate on a new dimension to the privacy problem – not only who we are and what we are doing, but also where we are doing it.”\(^ {316}\)


\(^{312}\) *The Privacy and Electronic Communications (EC Directive) Regulations 2003*, ibid, s 2(1).

\(^{313}\) *The Privacy and Electronic Communications (EC Directive) Regulations 2003*, ibid, s 2(1): “value added service means any service which requires the processing of traffic data or location data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication.”

\(^{314}\) *The Privacy and Electronic Communications (EC Directive) Regulations 2003*, ibid, s 14(2)-(5).


\(^{316}\) Bennett & Crowe, *ibid*. 
Also in 2005, the Surveillance Project at Queens University published a report to the OPC titled “Location Technologies: Mobility, Surveillance and Privacy.” The report noted:

LBS enables comprehensive surveillance practices that are designed for the purposes of influence, management, care and control to monitor any number of individuals or groups of individuals. In a highly mobile era, when capitalism is defined by its management of consumption, LBS make sense not only as conveniences but also as means of tracking, profiling and sorting different types of customers, travelers, workers, citizens and others.

In 2010, Professor Teresa Scassa posed “the threshold question for the application of data protection laws: when does information placed in a geographical context become personal information?”

Although personal information tends to be defined in Canadian data protection statutes as ‘information about an identifiable individual’, the case law has yet to reach a clear consensus on the standard for assessing when information is personal information. It suggests that some information linked to individuals is about them, while some is not. Yet the distinctions between the two kinds of information are sometimes difficult to draw. The situation is made more complicated when information permits inferences to be drawn about individuals. Decision-makers must be conscious of the distinction between actual and inferred information and may need to develop concrete guidance as to which inferences trigger data protection concerns and which are more properly the domain of other public policy measures.

The ‘identifiable individual’ also raises challenges with respect to information in a geographical context. There appear to be two competing tests at present in Canadian data protection law. The Pascoe test of a ‘reasonable expectation’ that an individual may be identified is well established in Ontario, and courts and adjudicators in other provinces have adopted this test. At the federal level, a competing ‘serious possibility’ of identification standard has emerged, and it is not clear to what extent this test is different from that in Pascoe. Neither test may be well suited to dealing with the proliferation of computerised data that is becoming available through a growing range of sources, and that may permit the reidentification of individuals in previously de-identified data sets, or that may alter, from one day to the next, the ‘reasonable expectation’ or the ‘serious possibility’ that individuals can be re-identified.

In 2011 Professor Scassa and Anca Sattler concluded that “there are gaps” in the legislative framework applicable to location information and called for “proactive policy guidance and strong enforcement measures.” In their view, the use of standard form contracts, with multiple links and complicated privacy policies is “not an effective method to give notice to consumers about the collection, use and disclosure of location information, particularly given its sensitive

318 Lyon et al, ibid at 5.
320 Scassa, ibid at 214.
nature”, and that the use of “default” settings also may undermine privacy protections by forcing consumers automatically into sharing information.322

**Stakeholder views**

In Rogers’s view, the rules pertaining to location, and OBA, are clear, but too inflexible. Rogers believes that “with technology ... you run a risk where you put hard and fast rules in when consumer preferences and tastes change. You have to be careful about creating regulatory rules that are too inflexible when technology is changing.”

In Professor Geist’s view, in response to the question about whether Canada’s privacy laws are sufficient to deal with location information, the answer is “On paper, probably yes, but in practical reality the answer is probably no.” In Professor Geist’s view, although location-data may have some positive uses, “location is highly personal,” and “aggregate data can still be misused.” Professor Geist anticipated that the OPC’s findings in the case of its investigation into Bell’s “Relevant Ads” program could provide some clarity on how the OPC interprets the law in relation to location information.

In the IPC-BC’s view PIPA (the BC statute substantially similar to PIPEDA) is “based on generally applicable privacy principles, which makes them capable of adapting and applying to new technologies as those technologies develop. In the recent Legislative Review of PIPA our office recommended against technology-specific amendments to that Act because of its ability to use general principles to address the privacy issues associated with new technologies.”

In Professor Steeves’s view, while PIPEDA is not inherently bad legislation in and of itself, PIPEDA was designed for bilateral exchanges of information, not the types of wide-ranging and often unknown multilateral collection and sharing and use of that information we see today. In her view, PIPEDA has been interpreted in a manner that supports “collection and commoditization” of personal information as the “default,” to the point where it seems PIPEDA failed to adapt to the state of technology where “everything is now collectable.” She says the technology, and the law, have failed to unbundle function-specific location sharing (e.g., providing location for a map) from broad-sweeping default collection of all information, and that the default favours large businesses, whereas the law disadvantages individuals who suffer from a huge power imbalance and information control limitations. In her view, businesses have been given too much freedom to collect personal information unrelated to specific purposes, and the resulting over-collection of data is being used in ways that are socially harmful, including marginalizing certain segments of the population who will not be able to receive certain goods and services as their profiles make them less attractive to corporations based on such demographic factors as income, location, and other habits.

322 Scassa & Sattler, *ibid* at 134.
Doctrinally, she says, any business “right” to collect information needs to be balanced by the state against individuals’ “right” to keep their information. In her view, PIPEDA has been interpreted in such a way as to be far more “commercial” in its approach to privacy, and that what is needed is a “human rights” approach to the privacy interests at stake. “The real question that needs to be asked: Have we developed an information infrastructure that’s created discriminatory and prejudicial impacts on certain groups within society? We need to look at the consequences of that information infrastructure, including untested benefits, and we need to think clearly about the broad claims about business interests that are being used to sacrifice our privacy.”

Professor Skillicorn shared a similar view, suggesting that the duty of the state is both to educate their citizenry, and protect them.

In his view, PIPEDA falls short when it comes to protecting privacy. He believes that PIPEDA’s focus is more on individual, discrete bits of information rather than the synthesis of that information. In his view, “for privacy, you have to be much more conservative about how you treat individual pieces of information so that the synthesis doesn’t defeat that. The problem is, the law is old and technology is [now] outstripping it.” In particular, “the blind spot that legislators have is how powerful inductive analytics can be. The possibility and the technology – that’s the challenge.” He stated his view that fundamentally, “personal information” is an “un-definable concept. You simply cannot tell if a given piece of information is personally identifiable – it certainly can’t be determined at the level of the data itself. It might be handled at the level of the process.”

Conclusion on legal protections

The discussion of privacy rights necessarily involves a consideration of the social goals underlying the legal rules (statute and common law) in place, as some of the stakeholders suggested.

Setting aside more foundational issues relating to whether PIPEDA strikes a right balance between potentially competing (social and business) interests, and the expressed “need” for businesses to collect information and the legislated “right of privacy of individuals,” the legal question remains whether PIPEDA sufficiently protects Canadians from location information being collected, used and shared. This hangs on whether the location-based information is “information about an identifiable individual,” which is determinative of a series of further obligations on behalf of the information seeker. While (as explored below) technological measures may play a role in de-personalizing the “personal” nature of personal information, this is not necessarily the desired safeguard. Fundamentally there is a greater issue about relative bargaining power, the ability of individuals to actually understand what is happening with their location information, and to in fact control the collection, use and disclosure of location-based personal information.
Requiring “consent” from the individual is that legal expression of control, and the nature of consent required has been interpreted generally to depend on the sensitivity of the information in question. Consent is also linked to the “specific purpose” for which the information is being collected. Given the wide-sweeping collection of information, often by unknown third parties, and often unknown to the individual, the “specific purpose” provision requires careful re-examination to ensure that it strikes the state’s desired balance between business interests and individual interests.

Failing that, consumers may be left to fend for themselves and that raises a question of whether the common law or statutory invasion of privacy cause of action (where recognized or where available) could be used to hold companies collecting and using location information to account. Some immediate hurdles to that approach, assuming the cause of action exists and applies in the context of location information, include that there would still be an enormous informational disadvantage to consumers who may not have sufficient information, or information at all, about their privacy being invaded, on top of the financial burden (expense) and risk (party costs) associated with litigation. Test cases will need to be brought forward before any clarity is available, and even then it may be that the courts turn to PIPEDA, and the OPC’s body of work, for guidance on the matter.

For the foreseeable future therefore it seems that PIPEDA will be the baseline against which the privacy of location information (and other personal information) is judged, placing the OPC in the central role.

Institutionally, the inability of the OPC to issue its own orders (instead of having to take the matter to the Federal Court) and impose fines for non-compliance may present a compliance challenge.

Scassa and Sattler have recommended “more and better enforcement tools” for the OPC, including the ability to “name and shame” organizations that have data security breaches, order-making powers, and the ability to impose “significant fines” on companies that do not properly handle personal information.323

Most recently, the OPC made issues findings in respect of an investigation into complaints about Bell’s “Relevant Ads” program (described above) which included a finding that due to the collection and use of potentially vast amounts of sensitive personal information, express consent was required. Of particular note, the OPC found that Bell had not properly explained to users what it meant by the term “location,” let alone in any detail. In weighing the sensitivity of the information and the reasonable expectations of the individual the OPC:

- further recommended that Bell obtain consent for any future uses of other information, including that related to mobile location or network usage for Bell Residential Services,

---

only once Bell is able to provide a sufficiently clear and detailed explanation of intended uses to support meaningful consent.\textsuperscript{324}

In the initial report on findings, the OPC noted that Bell had “[r]efused to comply” with the OPC’s recommendation. Shortly thereafter, Bell changed tack, and wrote to the OPC (as well as the CRTC), stating that Bell was suspending its program but that it would bring the program back on an opt-in basis. As Professor Michael Geist observed, prior to Bell’s decision to comply, the lack of order-making powers is problematic from an enforcement perspective:

Bell’s decision to violate Canadian privacy law leaves the Privacy Commissioner of Canada with little alternative: it must pursue the case in the Federal Court of Canada. Yet that approach will takes years as the case will have to be mounted from scratch. In the meantime, Bell will presumably continue to violate the law.\textsuperscript{325}

Indeed, the OPC itself had this to say in 2013:

The days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise. It is time to put in place financial incentives to ensure that organizations accept greater responsibility for putting appropriate protections in place from the start, and sanctions in the event that they do not. Without such measures, the Privacy Commissioner will have limited ability to ensure that organizations are appropriately protecting personal information in the age of Big Data.\textsuperscript{326}

As such, below it is recommended that the OPC be granted order-making and fining powers. The CRTC too has an important role to play, and one recognized by the OPC. TSPs play a central role, either passively (for app providers) or actively, in the collection and use of location information for technical and perhaps other purposes. Yet it appears that a full picture of what is actually taking place within the TSPs and between TSPs and app providers is missing. Therefore below is it recommended that the CRTC, the regulator of TSPs, initiate a fact-finding process about their collection, use and disclosure of location information.

\textsuperscript{324} The Privacy and Electronic Communications (EC Directive) Regulations 2003, \textit{ibid} at paras 112 and 115.


\textsuperscript{326} Office of the Privacy Commissioner of Canada, “The Case for Reforming the Personal Information Protection and Electronic Documents Act” (May 2013), online: <https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp>.
Chapter 5 – Technological, and self-regulatory (voluntary) approaches

This chapter highlights various technological, self-regulatory, and voluntary measures that are being promoted in the face of the growing use of location-based technologies, and growing concerns over privacy.

Technological approaches to protecting location information

Professor Scassa has identified various “technological data protection methods such as location anonymiser, cryptographic techniques, obfuscation or others”327 which could be used to protect consumers’ privacy. Another technological approach is through end-user software applications, for example the “Protect my Privacy”328 app. The focus of this report is on anonymization and de-identification, distinct329 but often-related techniques which appear to be a more common technological response to privacy concerns.

Anonymization is the term given to the process of removing components of a data set, such that the data set can no longer identify the users from which it was gathered. The goal of anonymization is to strike a balance between maintaining the usefulness of the data set and minimizing the privacy risks to the individuals represented in the data. However, not all methods of anonymization are equally effective, and a poorly-anonymized data set can still reveal personal details of individuals through “re-identification.”

For example, if a data set is composed of entries with four fields: (1) name, (2) address, (3) postal code and (4) location data point, it could be anonymized to two fields: (1) postal code, and (2) location data point. This appears to prevent knowing where an individual has been. However, if there is only one person in a given postal code in the data set, or if analysis of the data set reveals patterns in the location data, an individual could still be “re-identified” from the anonymized data set.

Anonymization, re-identification and their associated risks have been, and continue to be, an active area of academic, industry and public research.

Several researchers and institutions believe that anonymization is not an effective privacy safeguard in general, or specifically for location data. Professor Paul Ohm, for example,

329 See e.g. Gregory S. Nelson (ThotWave Technologies), “Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification” at 12.

De-identification of data refers to the process of removing or obscuring any personally identifiable information from individual records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. Anonymization of data refers to the process of data de-identification that produces data where individual records cannot be linked back to an original as they do not include the required translation variables to do so.
believes that the power of anonymization has been “vastly” overstated, and that it has given privacy regulators a false sense of ease due to re-identification actually being technically “easy.” The consequence is that there is now a broken promise of privacy law which has been “thoroughly infiltrated” by a belief in the power of anonymization. In Professor Ohm’s conclusion, “Clever adversaries can often reidentify or deanonymize the people hidden in an anonymized database.”

The OPC has noted that “anonymization can be challenging to achieve” and therefore recommended effective measures be put in place to render personal information anonymous and that personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.

A research group led by the Media Lab at the Massachusetts Institute of Technology published a study in 2013 that analyzed mobility data from 1.5 million individuals and concluded “human mobility traces are highly unique.” The study noted uniqueness decreased with coarser time or spatial resolution (e.g. instead of a latitude and longitude point at a specific time of day, a cell-tower sized area and a 1 or 2 hour time interval), however even with coarse data, unique paths could still be identified. The study did not identify particular individuals using the data set; however, the uniqueness of mobility data means that individuals can be easily identified when combined with an external data source:

A simply anonymized dataset does not contain name, home address, phone number or other obvious identifier. Yet, if individual’s patterns are unique enough, outside information can be used to link the data back to an individual. For instance, in one study, a medical database was successfully combined with a voters list to extract the health record of the governor of Massachusetts. In another, mobile phone data have been re-identified using users’ top locations. Finally, part of the Netflix challenge dataset was re-identified using outside information from The Internet Movie Database.

The risk of re-identification using external data sources is particularly relevant for location tracking using smartphones, since application developers are gaining access to smartphone


Easy reidentification represents a sea change not only in technology but in our understanding of privacy. It undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations. Regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from imminent, significant harm.

331 Ohm, ibid at 1703 [emphasis original].
332 Office of the Privacy Commissioner of Canada, “Policy Position on Online Behavioural Advertising” (June 2012) at FN 14, online: <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.
334 Montjoye et al, ibid.
GPS sensors, and smartphone users tend to publish information about themselves publicly on social media.

Even if the location data produced by a smartphone is anonymized before being sent to, for example, a smartphone app developer, the other sensors embedded in modern smartphones can contribute to re-identification of anonymized location data. Smartphones usually include a magnetic field sensor and an accelerometer, in addition to location-generating sensors, which can be used to generate further data on users:

For example, an analysis of magnetic field and acceleration data over a period of days yields information about the activities and movements of the user. If the user works in an office near a magnetic field and lives somewhere without one (which is not unlikely), the magnetic field sensor data could be used (in combination with other data) to deduce his or her location.

Example: The app Jigsaw is able to recognise user activities based on an analysis of microphone, GPS and accelerometer for patterns characteristic of routine activities. For example, the jolts produced when the user is walking depend on whether the phone is in a trouser or jacket pocket, so the software can recognise both patterns.335

On the other hand, some stakeholders believe that anonymization of personal information, when done correctly, is a sufficient answer to privacy concerns. Ann Cavoukian, former Information and Privacy Commissioner of Ontario (IPC-ON), has co-authored many papers on de-identification, arguing that it can be effective when implemented properly.336

For example, in a recent report on de-identification, Ann Cavoukian and Daniel Castro note that the removal of “direct identifiers” from a data set is generally seen as insufficient to protect a data set from re-identification, and the uniqueness of mobile data traces cannot be generalized to all other types of data.337 In direct response to the MIT Media Lab study described above, the report notes that despite the risks of re-identification the authors described, they did not in fact re-identify any individuals from their data set, nor describe a process of how to do so. Their 95% re-identification rate also depended on having four specific types of data points obtained from an external source on each individual in the data set before they could be identified. The report goes on to argue the other examples of re-identification using external data sets were poorly

---


anonymized, or legislative protections have been enacted that would prevent the same attack from occurring today.

The report notes that de-identification (i.e., anonymization) is often performed poorly, since it often reduces the analytical value of the data set.\textsuperscript{338} However, with a proper process and privacy concerns built into the data collection process, the risk of re-identification can be minimized while preserving the value of the data set. The report gives the example of the U.S. Heritage Health Prize competition, where a team proposed a three step anonymization process resulting in a re-identification risk of 0.84%, while preserving the analytical value of the health data.\textsuperscript{339}

In another paper, Cavoukian and Professor Khaled El Emam, whose research involves the development of de-identification standards for the use of health data for such uses as clinical trials, argued that “it is highly misleading to suggest that the re-identification of individuals from de-identified data is an easy task.”\textsuperscript{340} In those authors’ view, “If proper de-identification techniques and re-identification risk measurement procedures are used, re-identification remains a relatively difficult task.”\textsuperscript{341}

Shortly after the Cavoukian and Castro paper was published, another report criticizing their conclusions was published by researchers at Princeton University.\textsuperscript{342} The report noted 50% of the individuals in the MIT Media Lab’s study could be identified using only two data points, such as work address and home address, which can be easily obtained from data brokers. Further, the risks of re-identification increase with data sets that contain more and more data points on their users. In the modern data analysis industry, these data sets are common. The researchers also take issue with the U.S. Heritage Health Prize team’s calculations, saying that under a different set of assumptions, the re-identification rate could be as high as 12.5%.

The debate over anonymization’s effectiveness has not yet been settled, and best practices, to the extent that anonymization is accepted as a legitimate safeguard, have yet to be established.

\textit{Stakeholder views}

One of the problems identified in the stakeholder consultation was the collection of data by third parties, unbeknownst to users.

\textsuperscript{338} Cavoukian & Castro, \textit{ibid} at 9.
\textsuperscript{339} For a detailed review of re-identification studies in the health sector, see Khaled El Emam et al, “A Systematic Review of Re-Identification Attacks on Health Data” (2 December 2011), online: <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0028071>.
\textsuperscript{340} Ann Cavoukian (Information & Privacy Commissioner, Ontario) & Khaled El Emam, “Anonymization Remains a Strong Tool for Protecting Privacy” (June 2011).
\textsuperscript{341} Cavoukian & El Emam, \textit{ibid} at 15.
\textsuperscript{342} Arvind Narayanan & Edward W Felten, “No silver bullet: De-identification still doesn't work” (9 July 2014), online: <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.
In the stakeholder consultation, the OPC representative noted that “there are challenges with anonymization,” and noted that the US FTC\textsuperscript{343} has said, “There is always the possibility that ostensibly anonymized data can be re-identified.”\textsuperscript{344}

In the view of the IPC-BC, expressed in the stakeholder consultation, “If information is truly anonymized, then it is no longer personal information and further steps need not be taken. However, there is always a risk of re-identification of data, with this risk related to the sophistication of the initial measures to de-identify. This should be factored into any attempts at anonymization.”

Professor Skillcorn noted that “there is no such thing as ‘anonymized’ once you get beyond some trivial bits of information.” He said that

Huge numbers of websites are trying to figure out who you are, and many are for sure tracking you historically and through time and space and using that information. Online services know who your ISP is so they know roughly where you are connected from. Google is analyzing your online behavior and your emails, and possibly triangulating that with your ISP and also your comments online. Shared cookies and logic credentials are easy to correlate, and with more and more bits of discrete data gradually you can converge on a smaller and smaller radius, even someone checking email as they drive in to work, or use free wi-fi in a coffee shop.

Professor Steeves offered a similar view about the limitations of PIPEDA, arguing that “PIPEDA is really designed for bilateral exchanges of information,” not the extensive sharing of information and third party tracking that is becoming commonplace, nor the cloud-based storage of data. As Professor Steeves posed rhetorically: “How do I even consent to the cloud?”

**Self-regulatory approaches**

There have been a number of industry attempts to address privacy concerns on a voluntary basis, including transparency initiatives and self-regulatory codes.

**Transparency initiatives**

In response to growing concerns about privacy, some Canadian businesses (in line with a more global trend), including some telecommunications service providers\textsuperscript{345} and online service

\begin{footnotesize}
\begin{enumerate}
\item See FTC, *In the case of Compete, Inc*, online: <https://www.ftc.gov/enforcement/cases-proceedings/102-3155/compete-inc>.
\end{enumerate}
\end{footnotesize}
providers, have begun producing and publishing “transparency reports” in the context of providing information about the scale and scope of requests from government agencies, particularly law enforcement agencies, for subscriber information. At the same time, ongoing research has been revealing privacy weaknesses.

In March 2015, for example, two researchers released their “second annual report that evaluates the data privacy transparency of the most significant internet carriers serving the Canadian public.” That report concluded that:

- internet carriers generally show little interest in being transparent about key aspects of the handling of personal information;
- the internet carriers evaluated are generally not transparent in their handling of personal information, earning on average only 2 stars out of 10 possible;
- no carrier earned a full star in any of four criteria;
- only one company stood out by earning more than 5 stars; and
- many Canadian internet carriers are in violation of their legal responsibilities under PIPEDA.

The report made a number of recommendations to various stakeholders, including (i) amending PIPEDA’s Principle 8 — Openness to include proactive transparency around key privacy policies; and (ii) a recommendation to privacy commissioners and the CRTC to “more closely oversee carriers, Canadian and foreign, to ensure their data privacy transparency and compliance with legal obligations.”

**Self-regulatory codes**

There have been a number of attempts by industry to develop their own codes of behaviour.

In the United States, for example, the Future of Privacy Forum, together with Senator Charles Schumer, introduced an “MLA Code of Conduct” that is an enforceable, but self-regulatory framework. The code puts data protection standards in place to allow for responsible use of MLA technology. The code has five main goals that MLA companies must adhere to, which are: (1) providing detailed privacy notices on their website describing the type of information collected; (2) de-identifying and de-personalizing MAC addresses that have been collected; (3) ensuring that MLA data is only used for its intended purposes; (4) retaining collected MLA data

---


347 Clement & Obar, ibid at 8.

for a limited period of time; and (5) providing customers with the opportunity to opt out of being tracked by their mobile location.  

In Ontario the IPC-ON, in partnership with Aislelabs, a private sector MLA technology company, endorsed using the principles of “privacy by design,” in conjunction with the MLA Code of Conduct.  

The MLA Code of Conduct has been criticized for being too weak. The Electronic Frontier Foundation, a U.S. nonprofit organization whose focus is on “defending civil liberties in the digital world,” has stated that the MLA Code of Conduct “falls short of protecting consumers,” namely because (i) the opt-out nature of the program is onerous and unlikely to gain much “pick-up” from consumers, especially because (ii) it relies on notice from retailers involved in the tracking programs.

Although one might argue that the endorsement of the IPC-ON of the MLA Code of Conduct would have a binding effect on those subject to Ontario’s privacy law, whether that is the case remains to be seen, except the normative phrasing of the MLA Code of Conduct could be interpreted as only being aspirational and not obligatory. In any case, the above-referenced criticisms remain.

Another example of an industry effort to develop a self-regulatory code is the “Canadian Self-Regulatory Principles for Online Behavioural Advertising,” developed by the Digital Advertising Alliance of Canada, which describes itself as “a consortium of leading Canadian advertising and marketing associations.” According to the DAAC:

The Principles set out a consumer-friendly framework for the collection of online data in order to facilitate the delivery of advertising based on the preferences or interests of Web users, in a manner consistent with applicable Canadian privacy laws and the core elements of the Self-Regulatory Principles for Online Behavioural Advertising created by the Digital Advertising Alliance in the United States.

To the extent that the Principles are merely a statement of commitment to privacy law (i.e., normally PIPEDA) the Principles do not likely add any consumer protection. Thus, while the Principles state that “[e]ntities should not collect and use sensitive Personal Information for


350 Ann Cavoukian et al, “Building Privacy into Mobile Location Analytics (MLA) Through Privacy by Design” (March 2014) at 2, online: <https://www.ipc.on.ca/images/Resources/pbd-mla.pdf>.  

351 Electronic Frontier Foundation, “About EFF”, online: <https://www.eff.org/about>.  


Online Behavioural Advertising without consent, as required and otherwise in accordance with applicable Canadian privacy legislation,” the reader must then refer to Canadian privacy legislation (and guidance, all as discussed above in this report). Nowhere do the Principles specifically address location. Furthermore, the list of members appears small, with 44 companies (and only one TSP, Rogers) and eight associations.354

Conclusion on technological and self-regulatory (voluntary) approaches

There is an ongoing debate about the sufficiency of technological measures to protect consumers’ privacy, but it seems that the dialog may be too narrowly focussed around the legal definition of personal information (“information about an identifiable individual”), which fails to capture broader concerns about the social impacts of individuals being profiled and targeted based on deep behavioural insights inferred from information which appears to increasingly have a location element to it. This report is unable to settle that highly technical debate. Instead, this report recommends that, given the concerns Canadians have expressed about location information and the apparent extent to which location is now being sought as a highly valued piece of data for behavioural analytics, the OPC and the CRTC should study the issue in greater depth.

In light of the problems associated with unequal bargaining power, concerns with lack of transparency, and the practical inability to give informed consent in the face of lengthy, unread privacy and user agreements, or to consent to third parties unknown to end users, this report concludes that self-regulation (voluntary) approaches are an insufficient form of protection for highly personal, highly sensitive location data. For self-regulation to work, all collectors and users of data needed to be signatories to the code, an unlikely expectation in the absence of a mandate.

354 “Participating Companies” and “Participating Associations”, online: http://youradchoices.ca/participating-companies>.
Chapter 6 – Conclusion and recommendations

Based on the analysis in this report, it is not clear if Canada’s privacy regime is sufficiently responsive to Canadians’ concerns with location-based informational privacy.

The wide-scale collection, use and disclosure of location-based information, due to the context-specific nature of privacy law in Canada and the broad interpretation of the appropriate and specific purposes limitations, may be permissible at law so long as the information itself does not meet the test of being “personal information,” either in and of itself (on its own), or through technological measures which strip the information of its utility in identifying the individual.

The current privacy protections may not be sufficient for the purposes of balancing the privacy interests of individuals against the collection, use and disclosure of location-based information, particularly by third parties, for use for location-based marketing and the provision of location-based services. This is particularly the case where it may be accepted that so long as a person may not be identified as a result of the information, then the wide scale collection and use, including social sorting, is therefore acceptable.

A stronger default of privacy protection for location information, as seen in the European context, may therefore be required. This is because (i) the power imbalance between individuals and the businesses collecting and using the information is great; (ii) the identity of the entities (particularly third parties) collecting or using the information is often difficult if not impossible to ascertain; (iii) the disclosures too complex, time-consuming, and difficult to understand. People ought to, in their everyday lives (and subject to criminal law), be able to effectively be “off-the-grid”, and free from social sorting if they so choose, but it appears they cannot effectively do so.

Based on this analysis, and building on previous PIAC recommendations in respect of privacy matters, the following are therefore recommended:

---

355 See Public Interest Advocacy Centre, “No Such Thing as a Free Lunch: Consumer Contracts and ‘Free’ Services” (March 2014). Recommendations included bringing forth a statutory breach of confidence tort, and enhancing the investigative and enforcement powers of the Office of the Privacy Commissioner of Canada.

See also Public Interest Advocacy Centre, “A ‘Do Not Track List’ for Canada” (October 2009). The report makes several recommendations, including a requirement for consumer opt in consent to online tracking and behavioural targeted advertising. Greater transparency and consumer education are needed for tracking technologies and behavioural targeted advertising practices on the internet. Canadian legislators and regulators should begin studying the issue of online behavioural targeted advertising to catch up to American and European regulators, who have already begun considering how their regulatory frameworks protect their consumers on the internet. The Privacy Commissioner should review the existing Personal Information Protection and Electronic Documents Act to set out guidelines for how website operators can deploy behavioural advertisement technology in order to comply with the law and protect the privacy of Canadians. The Government should review existing privacy legislation and regulatory framework and bring forward new rules as necessary to ensure that these systems only operate on an explicit, informed, opt-in basis and that an effective enforcement mechanism with fines exists to punish marketers who operate outside the rules. Special consideration must also be given to the issue of behavioural advertising targeting children and young people.
Recommendation 1: The OPC should conduct further research into consumer awareness and expectations of mobile device location tracking.

Recommendation 2: The “appropriate purpose” and “specific purpose” provisions of PIPEDA should be strictly interpreted and enforced to limit the general collection of location-based information. Specifically, location-based information should only be collected for the purposes of providing users with services based on their location (such as mapping, recommendations, and marketing alerts), and only when consumers have explicitly consented to that collection and use, upon clear ex ante notice to consumers that their location information will be collected and used by specified entities including third parties.

Recommendation 3: PIPEDA should be amended to include “location” within the definition of “personal information,” or alternatively the OPC should provide explicit guidance about “location information” meeting the definition of “personal information.”

This report has established that location is highly unique, highly identifiable, and highly personal in nature, even when anonymized and aggregated.

PIPEDA’s definition of “personal information” should therefore be interpreted to include information about a person’s location in time and through time. The OPC’s Interpretive Bulletin on “personal information” (last updated in October 2013) notes that certain other types of similar, if not analogous, information is categorically “personal information,” including “forms of biometric information, such as fingerprints and voiceprints”; “[t]racking information collected from a Global Positioning System (GPS) placed in company vehicles” (since the information can be linked to specific employees driving the vehicles, the employees are identifiable even if they are not identified at all times to all users of the system); and IP addresses if they can be associated with an identifiable individual. Information collected through the use RFID tags to track and locate baggage, retail products, and individual purchases may constitute personal information.

Currently, and in the absence of explicit interpretive guidance from the OPC or the courts, whether or not location information meets the definition of “personal information” under PIPEDA is determined on a case-by-case contextual analysis which often looks to discrete pieces of data, not the aggregate, disparate pieces of information. Therefore the OPC may be unable to ex ante and categorically deem all location information, despite its uniqueness, its vulnerability to misuse, and its allure to marketers, as “personal information,” or “sensitive” personal information deserving of the strictest form of consent. In that case, PIPEDA’s definition of

356 Office of the Privacy Commissioner of Canada, “The Meaning of Personal Information” (October 2013), online: <https://www.priv.gc.ca/leg_c/interpretations_02_e.asp>.
“personal information” could be amended to explicitly include location in the definition of “personal information,” as proposed in the following text (amendments indicated by underscore):

“personal information” means information about an identifiable individual, including but not limited to information about an individual’s location in time and over time, including information about past location, current location, and predictive information about a person’s future location, but does not include the name, title or business address or telephone number of an employee of an organization.

**Recommendation 4: The OPC should produce clear guidance on the level of consent required from smartphone users before their location can be collected.**

This report has argued that location information appears to be prima facie “personal information” and therefore consent should be required for its collection, use and disclosure.

As explained, location information may be highly unique, highly identifiable, and highly personal in nature, even when anonymized and aggregated. Various Privacy Commissioner findings support this view. Nevertheless, the determination about whether location information is “personal information” remains based on a contextual, case-by-case analysis, and it may be that sufficient technological measures may be implemented to strip such information of its identifiable information, although this paper suggests that de-identification is not foolproof.

What is even less clear however is what level of consent ought to be required for collecting, using and disclosing location-based personal information, and in this regard, similar to the OPC’s guidance on online-behavioural marketing, the OPC should produce guidance about the appropriate level of consent required for location-based information.

**Recommendation 5: The CRTC should initiate a fact-finding process into the collection, use, and disclosure of location information by telecommunications service providers, either directly through information gleaned directly from customers’ network usage information, or indirectly through purchasing that data from app providers.**

While some telecommunications service providers under the authority of the CRTC have begun the practice of issuing transparency reports, the burden of identifying and understanding TSPs’ information collection, use and disclosure practices falls on individuals. In many cases, privacy policies are lengthy, complex, incomplete, and therefore difficult to understand. This report therefore recommends that the CRTC conduct a review of TSP privacy practices, broadly, and more specifically in respect of location-based information, including issuing interrogatories to TSPs which include the following:

- Do you collection information about your subscribers’ location?
- Do you purchase information about your subscribers’ location from third parties?
Do you share information about your subscribers’ location with third parties?

**Recommendation 6: Amend PIPEDA to give OPC order-making power and fining power.**

As described earlier, a number of authors and the OPC have expressed concern over the OPC having no order-making power and finding power. Instead, the OPC must rely on “naming and shaming,” and can only resort to an application to the Federal Court for enforcement. Companies that judge privacy findings too inconvenient or expensive can continue to operate in a privacy-violating manner. Therefore it is recommended that that OPC be given order-making power, and fining power, to enhance the OPC’s ability to bring about compliance with PIPEDA.

---


---
Appendix A – PIAC Summary of Environics Telephone Survey

This survey was commissioned by PIAC and carried out by Environics Research Group. The telephone survey was conducted among a national random sample of 2,000 adults comprising 1,003 males and 998 females 18 years of age and older, living in Canada, between the 10th and 21st of September, 2014. The margin of error for a sample of this size is +/- 2.19%, 19 times out of 20.
Q1 – use of smartphone/tablet

Do you own or ever use a portable wireless device that has a variety of applications on it—such as a ‘smartphone’ or a tablet (e.g. an IPad)?

(a) Yes; (b) No; (c) Don’t know

Figure 3. Ownership or use of smartphone/tablet; total, by age range, by family income

The Total responses show that smartphone use is very common in Canada at 66%, and has increased rapidly in the past few years; the CRTC’s Executive Director of Telecommunications stated in a senate committee that smartphone use in Canada was 38% in 2011 and 51% in 2012. Location-based services are therefore likely to be a new concept to many Canadians, or a concept that many have not yet fully thought through.

The age group and family income level categories are included based on the statistically significant differences within their category. There is a clear trend that the younger the Canadian, the more likely he or she has or uses a smartphone. It is somewhat surprising that usage drops off by 27% between the 45-59 and 60+ groups, a significantly higher drop-off than any other range. A similar trend emerges in the family income category, with expected results, that as income level rises, so too does smartphone/tablet use. The difference between the lowest quintile (42%) and the highest quintile (88%) of smartphone users, 46%, is enormous (though due to small sample size this 46% difference actually has a much larger margin of error, +/- 11.2%).

There is also a significant difference between those employed (78%) and those retired (35%) who own or use smartphones, but this is likely due to the same trends seen with age (not graphed here).
Q2 – perception of location tracking

When you use your smartphone or tablet—including your use of applications you have downloaded—do you think your physical location is always, sometimes, rarely or never being tracked or do you not know?

(a) Always; (b) Sometimes; (c) Rarely; (d) Never; (e) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

Figure 4. Perception of the frequency of location tracking; total, by age group

The Total result shows a large proportion of Canadians (30%) do not know whether or not they are subject to location tracking when using their smartphones. This trend is seen generally among each age group, with only Age 60+ being significantly different than the Total. Interestingly, the age 30-44 group seem to either be more aware of location tracking (smaller “Don’t know” proportion) or just more cynical (significantly more believe “Always/Sometimes” while “Never/Rarely” is statistically the same as the others).

Overall, Canadians clearly believe their physical location is being, or can be, tracked while they use their smartphones.

There is also a significant difference in results between those with differing education levels (recall the sample is composed of people 18+ who have/use a smartphone). People with a Public/High School...
Q3 – comfortableness with receiving location-based coupons

How comfortable would you be if you received offers from retailers on your smartphone based upon your location? For example, you receive an offer on a discounted cup of coffee from a coffee shop because you were in the neighbourhood of that coffee shop? Would you be?

(a) Very comfortable; (b) Somewhat comfortable; (c) Somewhat uncomfortable; (d) Very uncomfortable; (e) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

education are more likely to not know than those with higher education, and those with higher education are more likely to believe tracking is being done, suggesting a gap in understanding that could be remedied through an education campaign of some sort.

The Total result shows that Canadians are clearly not comfortable with receiving advertisements or coupons from retailers based on their location. Only 9% of total respondents said they were "Very Comfortable" with the idea, and overall, nearly 2/3 of all Canadians (65%) are uncomfortable with receiving these kinds of offers.

Figure 5. Comfortableness with receiving location-based coupons; total, by age group

360
Q4 – comfortableness with the idea of location being tracked

How comfortable are you with the idea that your telecommunications service provider, an application provider or a retailer may be tracking your location based on your smartphone or tablet use?

(a) Very comfortable; (b) Somewhat comfortable; (c) Somewhat uncomfortable; (d) Very uncomfortable; (e) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

Figure 6. Comfortableness with the idea of location being tracked; total, by age group

There were very few variations within specific groups of Canadians, other than age group (odd result: Albertans had an unusually low “Very Comfortable” response rate at 2% compared to 8-12% for other regions).

Younger Canadians tend to fall on the “Somewhat Comfortable” side whereas older Canadians tend to fall on the “Very Uncomfortable” side. The “Very Uncomfortable” response is also quite low among 18-29 year olds, statistically significantly below all other age groups as well as the Total of all Canadians.

The Total result shows that the vast majority of Canadians (77%) are uncomfortable with the general idea of their location being tracked based on the usage of a smartphone. There were even fewer significant
differences within specific groups than in Q3, other than those that could readily be linked to older vs. younger age.

The age group differences are much more muted in the results from this question than Q3, but still show a pattern: older age groups (45-59, 60+) are significantly more uncomfortable with the idea of location tracking than the 18-29 group. There is a significantly larger proportion of the older age group that chose "Very Uncomfortable", but interestingly these "more comfortable" 18-29 year olds were concentrated more in the "Somewhat Uncomfortable" category rather than being more evenly spread into one of the "Comfortable" categories. Younger Canadians may be more amenable to smartphone-based location tracking than their older peers, but they too are still not particularly comfortable with the idea.

Comparing the results of Q3 and Q4, it seems that the younger the age group, the more amenable Canadians are to smartphone-based location tracking if they can derive a personal benefit from the tracking (i.e., a coupon/offer for a product).

The trend in each of Q3 and Q4 is less comfortableness as age increases, but the difference is far more pronounced for receiving a coupon/offer than the general idea of location tracking. This could suggest Canadians simply do not understand the implications of their location being tracked, similar to how Canadians highly value privacy yet are the some of the most active Facebook users per capita in the world. Note the reduced sample sizes mean the margins of error are larger, and therefore only the broader trends are comparable.
Q5 – main concerns about location being tracked

What would be your main concerns, if any, about your location being tracked when you use your smartphone or tablet?

(a) Invasion of privacy/concerns about loss of privacy; (b) No-one’s business but mine; (c) Concerns about information being misused/sold/shared; (d) Personal safety/security/stalking; (e) Concerned about my location being known/being constantly tracked; (f) Don’t want additional texts/ads/messages; (g) It’s creepy/unsettling/Big Brotherish; (h) Just don’t like the idea [non-specific]; (i) I would turn it off/must be with my consent; (j) Identity theft/data security; (k) Risk of robbery when it’s known I’m away from home; (l) Could be useful in an emergency/accident; (m) Other; (n) None/no concerns; (o) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

Figure 8. Specific responses to main concerns over location being tracked; total 363

363 The results from this question show Canadians are mainly (32%) concerned with an invasion of privacy resulting from their location being tracked. Overall, Canadians are concerned with general privacy invasions more than they are concerned with specific harms resulting from privacy invasions; see Figure 9 below.

A small percentage (13%) of Canadians find no concern at all with location tracking. In looking at the demographic results, the only anomaly are Quebeckers/Montrealers, that are statistically far above the other regions/cities (21% vs. 9-13% by province, 21% vs. 8-9% by city) for a response of no concern.
In keeping with the trend of Q3 and Q4, Canadians seem to value privacy generally more than they value the effect of protection from specific harms resulting from a breach of privacy (though, general privacy concerns could include breaches). This could be due to the lack of information of specific harms that could result from location tracking; as seen in Q2, a significant percentage of Canadians still don’t fully understand location tracking issues, or as seen in Q1 there is still a large age gap in the adoption of mobile devices which have the capability for location tracking.

Figure 9. Main concerns of location being tracked, grouped by type of response; total

This chart shows the groupings of responses into general privacy concerns and specific harms (see the response corresponding to each letter under the survey question above).
Q6 – importance of consent before location tracking

How important is it to you that you are always asked to give your permission before a telecommunications provider or an application provider or a retailer can start tracking your location? Is it…?

(a) Very important; (b) Somewhat important; (c) Not very important; (d) Not at all important; (e) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

Figure 10. Level of importance for obtaining permission before location tracking; total 365

Clearly the results of this question show Canadians, who generally are concerned about privacy, want to be in control of whether their location is being tracked, before any tracking begins. Also the question phrased as “…that you are always asked…” implies that Canadians would only be comfortable with a high level of consent, likely informed, explicit, opt-in consent. Combining the top 2 and bottom 2 responses, 91% vs. 8% (at a 2.8% margin of error) provides very little leeway for concluding otherwise. This result is strengthened taking into account Q2 and Q3, where even though a large proportion of Canadians either don’t know how they feel about location tracking or are comfortable with receiving coupons based on location tracking, but still want to be in control of when the tracking occurs.

The results for this question are the second most consistent across all demographic characteristics of all questions in the survey.

---

365 Clearly the results of this question show Canadians, who generally are concerned about privacy, want to be in control of whether their location is being tracked, before any tracking begins. Also the question phrased as “…that you are always asked…” implies that Canadians would only be comfortable with a high level of consent, likely informed, explicit, opt-in consent. Combining the top 2 and bottom 2 responses, 91% vs. 8% (at a 2.8% margin of error) provides very little leeway for concluding otherwise. This result is strengthened taking into account Q2 and Q3, where even though a large proportion of Canadians either don’t know how they feel about location tracking or are comfortable with receiving coupons based on location tracking, but still want to be in control of when the tracking occurs.

The results for this question are the second most consistent across all demographic characteristics of all questions in the survey.
Q7 – approval of sanctions for lack of consent before location tracking

If a company—such as a telecommunications provider or application provider or a retailer—starts tracking a person’s location without first getting their permission, should that company be penalized or sanctioned in some way?

(a) Yes; (b) No; (c) Don’t know

Note: question posed to the subsample of those from Q1 who own or ever use a portable wireless device that has a variety of applications on it

Figure 11. Percentage of respondents approving of sanctions for entities tracking location without consent; total 366

The only interesting anomaly is those who identified as self-employed rated “Very Important” significantly higher than any other employment group other than homemaker (92% vs. 64-84%, but not the much larger margins of error).

366 A clear result from this question; the vast majority of Canadians believe entities should get consent before they do any location tracking (Q6) and likewise the vast majority of Canadians believe a violation of that principle should result in sanctions of some sort. There was almost no variation in the demographic-specific results for this question.